

**QIP SUBMISSION — TO BE REPLACED BY JOURNAL VERSION**

This is our QIP submission (under an older title) dated Oct. 15, 2013 and re-formatted for the arXiv posting (the numbering of references may be different from the original submission). Since our presentation at QIP, we have received many requests for the paper. This post will eventually be replaced by our journal version, which is slowly in production due to the authors' many other obligations. The journal version will contain the same technical results in this version but will include a new perspective of “Physical Randomness Extractors”. Besides at QIP, this view was also presented by Yaoyun Shi in “Untrusted Quantum Devices” at Simon’s Institute, Berkeley, on Jan. 15, 2014 ([link for video](#), [link for updated slides](#)), and by Xiaodi Wu in “Physical Randomness Extractors” at Institute for Quantum Information, Caltech, on Feb. 18, 2014.

We consider the Equivalence Lemma (Lemma 4.6) a fundamental principle and powerful tool for securely composing untrusted-device protocols. In particular, readers interested “unbounded randomness expansion” using a constant number of devices are encouraged to explore the Lemma’s immediate implications on the security of the “cross-feeding” composition studied by Fehr, Gelles, and Schaffner [arXiv:1111.6052]. A proof for such a secure composition was first announced by Coudron and Yuen [arXiv:1310.6755]. See Miller-Shi [arXiv:1402.0489] for a more detailed discussion.

# Robust device-independent randomness amplification from any min-entropy source

Kai-Min Chung\*      Yaoyun Shi<sup>†</sup>      Xiaodi Wu<sup>‡</sup>

October 15, 2013

## Abstract

We investigate the task of randomness amplification, in which a weak random source is converted into a near perfect random output using *untrusted* quantum devices *without* any additional randomness. We present the first quantum-secure protocol that is *robust*, i.e., tolerating a constant level of noise on each quantum operation, and works for *all min-entropy sources*. Previous protocols, of Gallego, Masanes, De La Torre, Dhara, Aolita, and Acín (*QIP 2013*) and of Colbeck and Renner (*Nature Physics*, **8**, 450, 2012), are not robust and work only for the restricted class of Santha-Vazirani sources.

Our protocol is obtained by composing quantum-proof strong randomness extractors and multiple copies of device-independent randomness expansion protocols. To the best of our knowledge, we are the first to exploit *composition* of device-independent protocols, which makes both our construction and analysis significantly simpler than previous protocols, and allows us to instantiate our protocol based on *any* randomness extractors and randomness expansion protocols. Additionally, by relying on recent randomness expansion protocols of Miller and Shi (*personal communication*), our protocols can output exponentially long certified randomness with exponentially small error (in the min-entropy of the source) and have (sub-)exponential improvements on efficiency over the protocol of Gallego *et al.*

**Keywords:** device-independent randomness amplification, min-entropy source

---

\*Institute of Information Science, Academia Sinica, Taiwan.

<sup>†</sup>Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48103, USA.

<sup>‡</sup>Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.

## Extended Abstract of the QIP Submission

**Background.** How can one be certain that a random source is indeed random? This question is of great significance not just intellectually but practically because randomness is an indispensable resource for modern sciences and technologies, such as in randomized algorithms, physics simulations, and secure communication. Even though quantum mechanics postulates intrinsic randomness in Nature, it appears rather difficult to guarantee that the randomness at hand is not biased or partially known to a untrusted party. This question of obtaining certified randomness has attracted extensive studies from both computer scientists and physicists, albeit from different directions as summarized below.

Pioneered by Blum [Blu86] in the 1980’s, computer scientists asked whether we can instead devise methods to turn weak sources to near perfect random sources, and rely on weakest necessary assumptions on the sources for ensuring the output randomness. This led to the deep and elegant subject of randomness extractors (e.g., [Vad07]). On the one hand, researchers have realized that the *smooth*-min-entropy (or quantum conditional min-entropy) of a source characterizes the maximum amount of classically (quantum-, respectively) secure extractable randomness [Zuc90, Ren05, RWW06]. Thus the question becomes whether one can extract close to  $k$  uniform bits from a source with  $k$ -bits of min-entropy. On the other hand, deterministic extraction, i.e. in the absence of additional randomness, is known to be impossible, as shown by Santha and Vazirani [SV84] for the Santa-Vazirani (SV) sources. To get around the impossibility results, computer scientists have settled with making additional *independence* assumptions, and aim for randomness extractor either with one additional short truly random seed, or from two or a few independent weak sources. In both settings, independence is crucial for randomness extraction to be possible. However, independence is again a strong assumption that is hard to guarantee in reality. Thus, it is natural to ask:

*Can the independence assumption for randomness extraction be replaced by weaker and ideally verifiable physics assumptions?*

Interestingly, such possibility has recently been raised in the seminal work of Colbeck and Renner 2012 [CR12]. They were, however, motivated by the question if there exists fundamentally random events in Nature. Violations of Bell Inequality would provide evidence of such existence, except that this evidence is valid under the assumption of perfect random choices for the measurement setups. To break this circular “freedom-of-choice” loophole, Colbeck and Renner asked: could weak randomness be “amplified” to near perfect randomness, so that as long as the world is not deterministic, we could still be convinced of the existence of full randomness by first amplifying the weak randomness, then use the resulting almost perfect randomness for observing Bell violations? Since the randomness-making ability of the amplifying process is yet to be verified, this is precisely an untrusted-device question. Colbeck and Renner modeled weak randomness’ as a sequence of events, each of which weakly depends on all other events. Mathematically they form precisely a SV source. They partially answered their own question by showing how to turn all SV sources of sufficient randomness to a near perfect random bit. They conjectured that an arbitrarily weak SV source can still be amplified. This conjecture was confirmed by Gallego *et al.*. They interpreted the result in a dichotomy theorem: either we can never experience randomness because of the world is deterministic, or we can be convinced of the existence of full randomness, as any weak randomness, modeled by arbitrarily weak SV sources, can be amplified to enable the certification of full randomness.

One can also interpret the device-independent randomness amplification protocol of Gallego *et al.* as performing “deterministic extraction” for SV sources using untrusted and physically separated devices. As there is no trust needed to grant to the devices, we only need to ensure that the devices are physically separated, which is verifiable, and that the existence of “honest” devices passing the

protocol with high probability, which can in turn rely on quantum mechanics (following the protocol design). It is now natural to ask the following more concrete question:

*Can we perform deterministic extraction for any min-entropy sources using untrusted and physically separated devices?*

We further argue that the above question also has physics importance in significantly strengthening the dichotomy theorem of Gallego *et al.*. Recall that the goal is to identify *minimal* assumptions for which certifying randomness is possible. Note that SV sources is a rather restrictive classes of weak randomness. A more appropriate model is the broader min-entropy sources, given that min-entropy is known to capture extractible randomness.

Finally, we discuss desired properties for randomness amplification protocols. First, for it to be possible to empirically perform the protocol, *robustness* is essential. That is to require that the protocol accepts with high probability even when the “honest” devices suffers from a small amount of noise. The protocol of Gallego *et al.* is not robust and the authors posed achieving robustness as an important open problem. Second, for the protocol to have any practical meaning, efficiency is also essential, which can be measured by, e.g., the number of devices needed and the runtime of the protocol. If no efficient amplification exists, it remains a possibility that even if full randomness can be certified in principle, it may be too far in the future to be experienced. Finally, for some applications such as cryptography, high quality randomness are often necessary, thus small (e.g., negligible) error is also desirable.

**Our Contribution and Techniques.** We provide affirmative answers to (almost all of) the aforementioned questions by constructing the first *robust* quantum-secure randomness amplification protocols for *any* min-entropy sources. At a high-level, our protocol is obtained by composing quantum-proof strong randomness extractors and multiple copies of device-independent randomness expansion protocols (or more accurately, what we called randomness certification protocols.) To the best of our knowledge, we are the first to exploit *composition* of device-independent protocols, which makes both our construction and analysis significantly simpler than previous protocols.<sup>1</sup>

As the first step, we formalize the notions of (device-independent) randomness amplification protocols and randomness certification protocols. We view the formalization as part of our contribution, which provides cleaner language and is crucial for us to reason about composition of device-independent protocols. Roughly speaking, the goal of a randomness certification protocol  $\Pi_{\text{cert}}$  is to *certify* full randomness generated by the devices using a *truly uniform seed*; in other words, if the seed is uniform to the devices and environment, when protocol  $\Pi_{\text{cert}}$  accepts, it should output close-to-uniform random bits *even conditioned on everything, such as the seed and the environment, except the devices*. We call  $\Pi_{\text{cert}}$  a *strong* randomness certification protocol if  $\Pi_{\text{cert}}$  can achieve the same goal, but start with some seed that is only uniform to the devices, while might be arbitrarily correlated with the environment.

**Theorem 1.1 (informal)** *Given any quantum-proof strong randomness extractor  $\text{Ext}$  and quantum-secure strong randomness certification protocol  $\Pi_{\text{cert}}$ , a quantum-secure randomness amplification protocol  $\Pi_{\text{amp}}$  for any min-entropy source can be obtained by composing  $\text{Ext}$  and  $\Pi_{\text{cert}}$  as illustrated in Fig. (2).*

Our construction of  $\Pi_{\text{amp}}$  consists of the following three steps. The first step, which is our key idea, is to turn the input weak source  $X$  into a *quantum somewhere random source*  $\mathbf{S}$ . In classical case, a

---

<sup>1</sup>In particular, our protocol can rely on bipartite non-local games and do not require the use of linear program or non-constructive objects (which are needed by Gallego *et al.*) in both constructions and analysis.

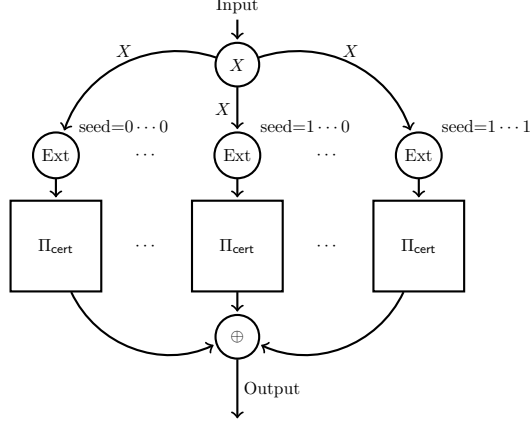


Figure 1: Illustration of Our Randomness Amplification Protocol.

somewhere random source  $\mathbf{S}$  is simply a sequence of random variables  $\mathbf{S} = (S_1, \dots, S_t)$  such that the marginal distribution of some block  $S_{i^*}$  is (close to) uniform (but there could be arbitrary correlation among them), which are useful intermediate objects for construction of randomness extractors (see, e.g., [Rao07, Li13]). It is not hard to see that one can turn a source  $X$  into a somewhere random source  $\mathbf{S}$  using a strong randomness extractor by simply letting  $S_i = \text{Ext}(X, i)$  for every possible seed  $i$ , and the property of extractor ensures that at least one block  $S_{i^*}$  (actually many of them) is close to uniform. We show that with appropriate definition, the same holds for quantum somewhere random source.

Our second step is to invoke a *strong* randomness certification protocol  $\Pi_{\text{cert}}$  to each block  $S_i$  with *distinct* set of devices  $\mathbf{D}_i$ , each of which outputs a decision bit  $O_i$  and a output string  $Z_i$ . By definition, when  $S_i$  is only uniform to the devices and  $O_i = \text{Acc}$ , we have that  $Z_i$  should be close to uniform *even when conditioned on everything except the device  $\mathbf{D}_i$*  (including, e.g.,  $S_i$  and  $S_j, \mathbf{D}_j$  from other blocks).

The protocol then accepts iff  $\forall i, O_i = \text{Acc}$ , and output  $Z = \bigoplus_i Z_i$  in that case. Intuitively, this could work since some  $S_{i^*}$  is close to uniform and thus if  $O_{i^*} = \text{Acc}$ , then  $Z_{i^*}$  is close to uniform *even conditioned on other  $Z_i$ 's with  $i \neq i^*$* , which implies  $Z = Z_{i^*} \oplus \left( \bigoplus_{i \neq i^*} Z_i \right)$  is close to uniform.

**Remarks.** For better understandings, it may be illustrative to note that simply outputting  $\bigoplus_i S_i$  would not work, due to the correlation among them. In contrast, we instead use each  $S_i$  to certify full randomness produced by each set of devices  $\mathbf{D}_i$ , which breaks the correlation among the blocks (in  $Z_i$ 's) and makes the XORing work.

To that end, our argument vitally relies on the fact that  $\Pi_{\text{cert}}$  is a strong randomness certification protocol. This is because to conclude that  $Z_{i^*}$  is close to uniform even conditioned on  $Z_{-i^*}$ , we need to deal with the case that  $S_{i^*}$  is independent of  $\mathbf{D}$  but might be correlated with the environment, which includes all blocks of  $S_i$  that  $i \neq i^*$ .

Our argument then follows from a sequence of non-trivial (though standard) quantum arguments for composition, one of which is to address the subtlety that the block  $S_{i^*}$  is only close to uniform, but not exact uniform, by using a fidelity preservation trick.

It is also worth noting that one interpretation of our framework is to reduce the task of randomness

amplification to a significantly simpler task of strong randomness certification where uniformly random sources are available for certifying randomness. In contrast, previous works of Colbeck and Renner and Gallego *et al.* attacks the amplification problem directly, and as such, are required to solve the certification problem with SV sources, resulting in significantly complicated protocols and analysis.

**Randomness Certification Protocols.** To instantiate protocol  $\Pi_{\text{amp}}$ , we need to find concrete randomness certification protocols. It is interesting to observe known quantum-secure DI-RE and DI-QKD protocols of Vazirani and Vidick [VV12a, VV12b] are randomness certification protocols. A very recent result of Miller and Shi [MS13] for quantum-secure randomness expansion also provides a novel randomness certification protocol that is *robust* and can certify *arbitrarily long* uniform randomness. It is worth mentioning that these protocols actually achieves much stronger goals than the one of randomness certification protocols.

The only issue with these protocols is that they are not *strong* randomness certification protocols by definition. Our another contribution in this paper is to prove that regular randomness certification protocols are also *strong* randomness certification protocols in a black-box way. This further reduces our task of finding reasonable randomness certification protocols. By plugging parameters from Miller and Shi’s protocol [MS13], we have

**Corollary 1.2 (informal)** *There exists a robust quantum-secure randomness amplification protocol that has polynomial runtime (in the length of the source) but with inverse polynomial error; there exists another robust quantum-secure randomness amplification protocol that achieves exponentially small error (in the min-entropy of the source) but not efficient.*

Full paper attachment to the QIP Submission



# 1 Background

How can one be certain that a random source is indeed random? This question is of great significance not just intellectually but practically because randomness is an indispensable resource for modern sciences and technologies, such as in randomized algorithms, physics simulations, and secure communication. Even though quantum mechanics postulates intrinsic randomness in Nature, it appears rather difficult to guarantee that the randomness at hand is not biased or partially known to a untrusted party. This question of obtaining certified randomness has attracted extensive studies from both computer scientists and physicists, albeit from different directions as summarized below.

Computer scientists asked whether we can instead rely on weakest necessary assumptions on the sources and design ways to turn weak sources to truly random sources, which leads to the beautiful subject of randomness extractors (e.g., [Vad07]). On one hand, people soon realized that *min-entropy* is the right measure for the amount of extractable randomness [Zuc90], so the question becomes whether one can extract close to  $k$  uniform bits from a source with  $k$ -bits of min-entropy. On the other hand, without any help of additional randomness, impossibility of deterministic extraction can be readily established even for restricted classes of sources such as Santa-Vazironi sources [SV84] (SV source for short). To get around the impossibility results, computer scientists has settled with making additional *independence* assumptions, and aim for randomness extractor either with one additional short truly random seed, or from two or a few independent weak sources. In both settings, independence is crucial for randomness extraction to be possible. However, independence is again a strong assumption that is hard to guarantee in reality. Thus, it is natural to ask:

*Can the independence assumption for randomness extraction be replaced by weaker and ideally verifiable physics assumptions?*

Interestingly, such possibility has recently been raised by the seminal works of Colbeck and Renner 2012 [CR12] and Gallego *et al.* [GMdIT<sup>+</sup>12] from physics motivations. Colbeck and Renner and Gallego *et al.* are motivated by the possibility of empirically certifying quantum mechanics through witnessing Bell violation that is known to be blocked by several theoretical “loopholes.” A particularly relevant one for us is so called “freedom-to-choice” loophole, which states that in order to witness Bell violation, the inputs to the non-local game are required to be *uniform* and *independent* of the system. Indeed, if our world is “super-deterministic,” namely no randomness, then even if quantum mechanics were true, we could not hope for certifying it at all. Colbeck and Renner and Gallego *et al.* then asks what is the minimal assumption for this to be possible, and aim for proving the following dichotomy theorem: either (i) the world is super-deterministic, or (ii) the world permits “weak freedom-to-choice,” which in turn implies certifiable full randomness. Both works modeled “weak freedom-to-choice” as the existence of a physical system that produce a single “mildly free bit,” and thus a sequence of such systems yield a SV source. Then, Gallego *et al.* constructed a *device-independent randomness amplification protocol* that converts any SV sources into a *certified* fully random bit using *untrusted* and physically separated devices, such that it guarantees that if the protocol accepts with not-too-small probability, then the output bit is close to uniform when the protocol accepts. As such, assuming the existence of physical devices that makes the protocol accept with high probability, Gallego *et al.* proved the dichotomy theorem when “weak freedom-to-choice” is modeled in a way that enables the existence of SV sources.

One can also interpret the device-independent randomness amplification protocol of Gallego *et al.* as performing “deterministic extraction” for SV sources with the help of untrusted and physically separated devices. As there is no trust needed to grant to the devices, we only need to ensure that

the devices are physically separated, which is verifiable, and that the existence of “honest” devices passing the protocol with high probability, which can in turn rely on quantum mechanics (following the protocol design). It is now natural to ask the following more concrete question:

*Can we perform deterministic extraction for any min-entropy sources with the help of untrusted and physically separated devices?*

We further argue that the above question also has physics importance in significantly strengthening the dichotomy theorem of Gallego *et al.*. Recall that the goal is to identify *minimal* assumptions for which certifying randomness is possible. Modeling “weak freedom-to-choice” as systems producing “mildly free bits” requires many distinct systems such that no two of them are fully correlated, which is arguably a strong assumption. In contrast, assuming the existence of a system that produce a string with sufficient min-entropy seems to be significantly weaker. On a more technical level, SV sources is a rather restrictive classes of sources. Assuming a world with weak min-entropy source is significantly weaker than assuming a world with reliable SV sources (at least in our eyes).

Finally, we discuss desired properties for randomness amplification protocols. First, for it to be possible to empirically perform the protocol in labs, *robustness* is essential, which requires the protocol to accept with high probability even when the “honest” devices suffers a small amount of noise. Indeed, the protocol of Gallego *et al.* is not robust and the authors post achieving robustness as an important open problem. Second, for the protocol to have any practical meaning, efficiency is also essential, which can be measured by, e.g., the number of devices needed and the runtime of the protocol. Finally, for some applications such as cryptography, high quality randomness are often necessary so small (e.g., negligible) error is also desirable.

## 2 Our Contribution and Techniques

We provide affirmative answers to (almost all of) the aforementioned questions (except achieving all desired property simultaneously) by constructing the first *robust* quantum-secure randomness amplification protocols for *any* min-entropy sources. At a high-level, our protocol is obtained by composing quantum-proof strong randomness extractors<sup>2</sup> and (multiple copies of) device-independent randomness expansion protocols (or more accurately, what we called randomness certification protocols). To the best of our knowledge, we are the first to exploit *composition* of device-independent protocols, which makes both our construction and analysis significantly simpler than previous protocols,<sup>3</sup> and allows us to instantiate our protocol based on *any* randomness extractors and randomness expansion protocols to optimize over different parameters.

At a high level, our composition framework can be viewed as reducing the task of randomness amplification to a significantly simpler task of *randomness certification* (defined shortly). As the first step, we formalize the notions of (device-independent) randomness amplification protocols and randomness certification protocols. We view the formalization as part of our contribution, which provides precise and cleaner language and is crucial for us to reason about composition of device-independent protocols. We refer the readers to Section 4 for further discussion.

---

<sup>2</sup>Recall that a function  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  is a quantum-proof strong randomness extractor, if for all source  $X$  that has sufficient min-entropy with respect to the environment  $E$ ,  $\text{Ext}(X, Y)$  is close to uniform with respect to  $Y$  and  $E$ , where  $Y$  is a uniform seed independent of  $X$  and  $E$ .

<sup>3</sup>In particular, our protocol can rely on bipartite non-local games and do not require the use of linear program or non-constructive objects (which are needed by Gallego *et al.*) in both constructions and analysis. See more in Remark 7.2.

Recall that the goal of a randomness amplification protocol  $\Pi_{\text{amp}}$  is to convert any weak source  $X$  with sufficient min-entropy to certified full randomness using untrusted devices; more precisely, if the source  $X$  has *sufficient min-entropy* with respect to the devices and environment, when  $\Pi_{\text{amp}}$  accepts, it should output close-to-uniform random bits with respect to the source  $X$  and the environment.<sup>4</sup> The goal of a randomness certification protocol  $\Pi_{\text{cert}}$ , instead, is to certify full randomness generated by the devices using a *truly uniform seed*; more precisely, if the seed  $X$  is *uniform* to the devices and environment, when  $\Pi_{\text{cert}}$  accepts, it should output close-to-uniform random bits with respect to the seed  $X$  and the environment. (We remark that here we make a stronger requirement that the output to be close to uniform with respect to both  $X$  and the environment, as opposed to just the environment. This is crucial for us to analyze the composition; see further discussion below.) Clearly, the later is a strictly simpler task as the source is guaranteed to be uniform. Our main construction shows how to construct the former from the later.

**Theorem 2.1 (informal)** *Given any quantum-proof strong randomness extractor  $\text{Ext}$  and randomness certification protocol  $\Pi_{\text{cert}}$  (with appropriate parameters), there exists a randomness amplification protocols  $\Pi_{\text{amp}}$  for any min-entropy source (with corresponding parameters).<sup>5</sup>*

Our construction of  $\Pi_{\text{amp}}$  consists of the following two simple steps (see Figure 2 for a pictorial illustration). The first step, which is our key idea, is to turn the input weak source  $X$  into a *quantum somewhere random source*  $\mathbf{S}$ . In classical case, a somewhere random source  $\mathbf{S}$  is simply a sequence of random variables  $\mathbf{S} = (S_1, \dots, S_t)$  such that the marginal distribution of some block  $S_{i^*}$  is (close to) uniform (but there could be arbitrary correlation among them). It is not hard to see that one can turn a source  $X$  into a somewhere random source  $\mathbf{S}$  using a strong randomness extractor by simply letting  $S_i = \text{Ext}(X, i)$  for every possible seed  $i$ , and the property of extractor ensures that at least one block  $S_{i^*}$  (actually many of them) is close to uniform. We show that with appropriate definition, the same holds for quantum somewhere random sources.

Our second step is to invoke a randomness certification protocol  $\Pi_{\text{cert}}$  to each block  $S_i$  with *distinct* set of devices  $\mathbf{D}_i$ , each of which outputs a decision bit  $O_i \in \{\text{Acc}, \text{Rej}\}$  and a output string  $Z_i$ . The protocol then accepts iff  $\forall i, O_i = \text{Acc}$ , and output  $Z = \bigoplus_i Z_i$  in that case. Intuitively, this could work since some  $S_{i^*}$  is close to uniform and thus by the property of randomness certification protocols, if  $O_{i^*} = \text{Acc}$ , then  $Z_{i^*}$  is close to uniform with respect to the environment, which implies that  $Z = Z_{i^*} \oplus \left( \bigoplus_{i \neq i^*} Z_i \right)$  is also close to uniform.

However, one needs to be careful in arguing the last step. To see the subtlety, it is helpful to note that while  $S_{i^*}$  is close to uniform,  $\bigoplus_i S_i$  is not necessarily close to uniform, due to the correlation among them. The key insight here, which is also the point of using randomness certification protocols, is that we can think of the environment of  $\Pi_{\text{cert}}(S_{i^*}, \mathbf{D}_{i^*})$  consisting of the remaining blocks  $S_{-i^*}, \mathbf{D}_{-i^*}$ , and thus  $Z_{i^*}$  being close to uniform with respect to the environment implies that  $Z_{i^*}$  is close to *even conditioned on all other*  $Z_{-i^*}$ , which is sufficient to imply that  $Z = Z_{i^*} \oplus \left( \bigoplus_{i \neq i^*} Z_i \right)$  is close to uniform.

However, there is another subtlety from the above argument. Note that if we think of the environment of  $\Pi_{\text{cert}}(S_{i^*}, \mathbf{D}_{i^*})$  containing  $S_{-i^*}, \mathbf{D}_{-i^*}$ , then  $S_{i^*}$  is no longer close to uniform with respect to the environment, due to the correlation between  $S_{i^*}$  and  $S_{-i^*}$ . Nevertheless, note that  $S_{i^*}$  remains

<sup>4</sup>Technically, we are slightly oversimplifying here (ignoring the case that the protocol accept with tiny probability) for cleaner description.

<sup>5</sup>See Theorem 6.1 for a formal statement with precise parameters.

close to uniform with respect to the devices  $\mathbf{D}_{-i^*}$ , and as such, we may still hope that  $S_{i^*}$  can still be used to certify the randomness produced by  $\mathbf{D}_{i^*}$ . More precisely, we need a *strong* randomness certification protocol  $\Pi_{\text{cert}}$  that if the seed  $S_{i^*}$  is *uniform* to the devices (but may correlated with the environment), when  $\Pi_{\text{cert}}$  accepts, it should output close-to-uniform random bits with respect to the environment.

Interestingly, we show that the two definitions are in fact *equivalent*, namely, any protocol  $\Pi_{\text{cert}}$  satisfies the weaker property implies that it also satisfies the stronger property. This thus allows us to conclude that the output of  $\Pi_{\text{amp}}$  is close to uniform when  $\Pi_{\text{amp}}$  accepts. We remark that here we crucially rely on the fact that the output is close to uniform with respect to both the source and the environment to prove the equivalence.

**Instantiations of Our Protocol.** To instantiate our main protocol  $\Pi_{\text{amp}}$ , we need to find concrete strong randomness extractors and randomness certification protocols. For randomness extractors, we rely on two extractors from the work of De et al. [DPVR12] (to optimize different parameters). For randomness certification protocols, it is interesting to observe that known quantum-secure DI-RE and DI-QKD protocols of Vazirani and Vidick [VV12a, VV12b] are both randomness certification protocols per our definition, and thus plugging in [VV12a] yields a protocol with exponential output length but is not robust, and relying on [VV12b] yields a robust protocol with linear output length. A very recent result of Miller and Shi [MS13] for quantum-secure randomness expansion also provides a novel randomness certification protocol that is *robust* and can certify *arbitrarily long* uniform randomness. Aiming for optimizing robustness, we additionally construct a new randomness certification protocol that tolerate 1.747% noise rate, at the price of only outputting a single bit. Relying on the extractors of [DPVR12] and the protocol of [MS13] and ours, we obtain the following corollary (see Section 7 for detailed discussion).

**Corollary 2.2 (informal)** *There exists (i) a robust quantum-secure randomness amplification protocol that has polynomial runtime (in the length of the source) but with inverse polynomial error, (ii) a robust quantum-secure randomness amplification protocol that achieves exponentially small error (in the min-entropy of the source) but has quasi-polynomial runtime in the input length and inverse of the error, and (iii) a robust quantum-secure randomness amplification protocol with polynomial runtime and inverse polynomial error that tolerate 1.747% noise rate and output a single bit.*

**Related Work:** We note that there are a few independent recent studies on randomness amplification protocols related to SV-sources (e.g., [GHH<sup>+</sup>13, MP13, RBG<sup>+</sup>13]). In particular, the work in [RBG<sup>+</sup>13] achieves an randomness amplification protocol for SV-sources with a certain robustness, which depends on the quality of the source.

**Organization:** we summarize necessary notation and concepts in Section 3. Then we proceed to the formal definition of randomness amplification protocols and randomness certification protocols in Section 4. We define and survey a few properties of quantum somewhere random sources in Section 5. Our main theorem of constructing randomness amplification protocols from randomness certification protocols is proved in Section 6. In Section 7, we discuss a few instantiations of our randomness amplification protocols by using different protocols as randomness certification protocols. We devote Appendix A and Appendix B to a concrete construction of a strong randomness certification protocol from BHK games.

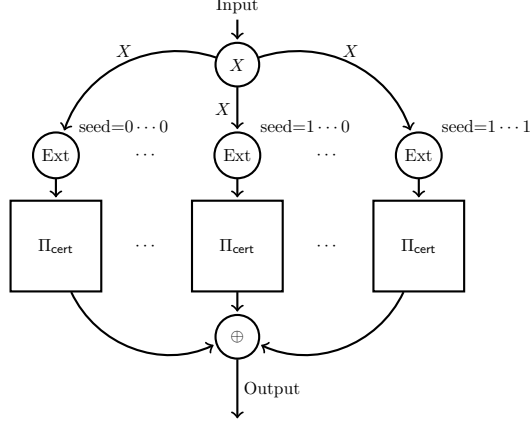


Figure 2: Illustration of Our Randomness Amplification Protocol.

### 3 Preliminaries

We assume familiarity with standard concepts from quantum information and summarize our notation as follows.

**Vectors.** For any vector  $x \in \mathbb{R}^n$ , we define  $|x|$  as the *point-wise* absolute value of  $x$ , namely,  $|x| = (|x_1|, \dots, |x_n|)$ . Similarly, for any two vectors  $x, y \in \mathbb{R}^n$ , we define  $x \preceq y$  as the point-wise inequalities  $x_i \leq y_i, \forall i \in [n]$  where  $[n]$  denotes the set  $\{1, \dots, n\}$ .

**Quantum States.** The state space  $\mathcal{A}$  of  $m$ -qubit is the complex Euclidean space  $\mathbb{C}^{2^m}$ . An  $m$ -qubit quantum state is represented by a density operator  $\rho$ , i.e., a positive semidefinite matrix with trace 1, over  $\mathcal{A}$ . The set of all quantum states in  $\mathcal{A}$  is denoted by  $\text{Dens}(\mathcal{A})$ . The Hilbert-Schmidt inner product on the operator space of  $\mathcal{A}$  (denoted  $L(\mathcal{A})$ ) is defined by  $\langle X, Y \rangle = \text{tr}(X^*Y)$  for all  $X, Y \in L(\mathcal{A})$ , where  $*$  is the adjoint operator.

For any multi-partite state, e.g.  $\rho_{ABE} \in \text{Dens}(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{E})$ , its reduced state on some subsystem is represented by the same state with the corresponding subscript, e.g. the reduced state on  $\mathcal{A}$  system is represented by  $\rho_A = \text{tr}_{\mathcal{BE}}(\rho_{ABE})$ .

We use  $|\psi\rangle$  to denote the density operator (i.e.,  $|\psi\rangle\langle\psi|$ ) of the pure state  $|\psi\rangle$  when it is clear from the context. Moreover, let  $\mathcal{U}_A$  denote the maximum mixed state on any space  $\mathcal{A}$ , i.e.,  $\mathcal{U}_A = \frac{1}{\dim(\mathcal{A})}\text{id}_{\mathcal{A}}$ , where  $\text{id}_{\mathcal{A}}$  denotes the identity operator over  $\mathcal{A}$ .

**Norms.** For any  $X \in L(\mathcal{A})$  with singular values  $\sigma_1, \dots, \sigma_d$ , where  $d = \dim(\mathcal{A})$ , the trace norm of  $\mathcal{A}$  is defined  $\|X\|_{\text{tr}} = \sum_{i=1}^d \sigma_i$ . The trace distance between two quantum states  $\rho_0$  and  $\rho_1$  is defined as  $\|\rho_0 - \rho_1\|_{\text{tr}}$ . Another important distance measure, *quantum fidelity*, between two quantum states  $\rho_0, \rho_1$  (denoted  $F(\rho_0, \rho_1)$ ) is defined as

$$F(\rho_0, \rho_1) = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_{\text{tr}}, \quad (3.1)$$

and admits the following connection with the trace distance.

**Lemma 3.1 (Fuchs-van de Graaf)** For any  $\rho_0, \rho_1 \in \text{Dens}(\mathcal{A})$ , we have

$$1 - \frac{1}{2} \|\rho_0 - \rho_1\|_{\text{tr}} \leq F(\rho_0, \rho_1) \leq \sqrt{1 - \frac{1}{4} \|\rho_0 - \rho_1\|_{\text{tr}}^2}. \quad (3.2)$$

Moreover, the fidelity between subsystems of quantum states could be preserved in the following sense.

**Lemma 3.2 ([JUW09, Lemma 7.2])** Let  $\rho, \xi \in \text{Dens}(\mathcal{A})$  and  $\rho' \in \text{Dens}(\mathcal{A} \otimes \mathcal{B})$  be density operators with  $\text{tr}_{\mathcal{B}} \rho' = \rho$ . There exists a density operator  $\xi' \in \text{Dens}(\mathcal{A} \otimes \mathcal{B})$  with  $\text{tr}_{\mathcal{B}} \xi' = \xi$  and  $F(\rho', \xi') = F(\rho, \xi)$ .

**Quantum Operations.** Super-operators from  $\mathcal{X}$  to  $\mathcal{Y}$  are linear mappings of the following form

$$\Psi : \text{L}(\mathcal{X}) \rightarrow \text{L}(\mathcal{Y}).$$

Physically realizable *quantum operations* are represented by *admissible* super-operators that are completely positive and trace-preserving. Thus any quantum protocol could be viewed as an admissible super-operator. We shall use this abstraction in our analysis and make use of the following observation.

**Fact 3.3 (Monotonicity of trace distances)** For any admissible super-operator  $\Psi : \text{L}(\mathcal{X}) \rightarrow \text{L}(\mathcal{Y})$  and  $\rho_0, \rho_1 \in \text{Dens}(\mathcal{X})$ , we have

$$\|\Psi(\rho_0) - \Psi(\rho_1)\|_{\text{tr}} \leq \|\rho_0 - \rho_1\|_{\text{tr}}.$$

For the convenience of our analysis, we define the following admissible super-operator:

**Definition 3.4 (“uniform” super-operator)** Let  $\Phi_{\text{unif}}^A(\cdot) : \text{L}(\mathcal{A}) \rightarrow \text{L}(\mathcal{A})$  be a super-operator such that for any classical-quantum state  $\rho_{AB} \in \text{Dens}(\mathcal{A} \otimes \mathcal{B})$  ( $\mathcal{A}$  classical,  $\mathcal{B}$  quantum),

$$\Phi_{\text{unif}}^A \otimes \text{id}_{\mathcal{B}}(\rho_{AB}) \stackrel{\text{def}}{=} \mathcal{U}_A \otimes \text{tr}_A(\rho_{AB}).$$

**Min-entropy.** For any c-q state  $\rho_{XE}$ , the amount of *extractable* randomness of some source is characterized by the (*smooth*) *conditional min-entropy*.

**Definition 3.5 (conditional min-entropy)** Let  $\rho_{XE} \in \text{Dens}(\mathcal{X} \otimes \mathcal{E})$ . The min-entropy of  $X$  conditioned on  $E$  is defined as

$$H_{\infty}(X|E)_{\rho} \stackrel{\text{def}}{=} \max\{\lambda \in \mathbb{R} : \exists \sigma_E \in \text{Dens}(\mathcal{E}), \text{s.t. } 2^{-\lambda} \text{id}_X \otimes \sigma_E \geq \rho_{XE}\}.$$

We can also consider the *smooth* min-entropy that consists in maximizing the min-entropy over all sub-normalized states that are  $\epsilon$ -close to the actual state  $\rho_{XE}$  in trace distance. Note that allowing an extra error  $\epsilon$  could increase the min-entropy of a certain state very significantly.

**Definition 3.6 (smooth min-entropy)** Let  $\epsilon \geq 0$  and  $\rho_{XE} \in \text{Dens}(\mathcal{X} \otimes \mathcal{E})$ , then the  $\epsilon$ -smooth min-entropy of  $X$  conditioned on  $E$  is defined as

$$H_{\infty}^{\epsilon}(X|E)_{\rho} \stackrel{\text{def}}{=} \max_{\|\sigma_{XE} - \rho_{XE}\|_{\text{tr}} \leq \epsilon} H_{\infty}(X|E)_{\sigma},$$

## 4 Model Definition

In this section, we formalize the tasks of randomness amplification and randomness certification protocols. We start by defining the syntax of protocols and stating the physics assumptions on the devices.

**Syntax and Assumptions.** A *protocol*  $\Pi$  is a classical algorithm that given an input string  $x \in \{0, 1\}^*$  (drawn from some source  $X$ ) and black-box access to a set of devices  $\mathbf{D} = (D_1, \dots, D_t)$  (i.e.,  $\Pi$  can make (multiple) classical queries to and receive classical outputs from each device), outputs a decision bit  $o \in \{\text{Acc}, \text{Rej}\}$  that indicates acceptance/rejection and an output string  $z \in \{0, 1\}^*$ . The input/output behavior of a device is referred to as the *strategy* of the device. The protocol execution is denoted by  $(o, z) \leftarrow \Pi(x, \mathbf{D})$ .

We consider the standard device-independent setting where the devices  $\mathbf{D}$  are prepared by a (potentially adversarial) environment  $E$  and require the security property to hold against  $E$  (e.g., output being uniform). Additionally, we emphasize that we allow *arbitrary* correlation between the source  $X$  and  $(\mathbf{D}, E)$ , as long as, e.g.,  $X$  conditioned on  $\mathbf{D}$  has sufficient min-entropy for randomness amplification. We make the following two (standard) physics assumptions.

- We assume that both the environment and the inner workings of the devices  $\mathbf{D}$  are quantum. Hence, the initial state of the protocol can be described by a CQQ state  $\rho_{X\mathbf{D}E}$ , and the strategy of each device can be fully specified by their initial state and a sequence of POVMs.
- We assume that during the protocol execution, all devices and Eve are physically separated from each other and hence there is no signaling among them.

Following the above assumptions, we can abstract the protocol execution as an *admissible* super-operator  $\Psi_\Pi : \mathcal{L}(\mathcal{X} \otimes \mathbf{D}) \rightarrow \mathcal{L}(O \otimes \mathcal{Z} \otimes \mathcal{X})$  (determined by the protocol  $\Pi$  and the inner workings of the devices  $\mathbf{D}$ , and keeping a copy of the classical source  $X$ ) applied to the  $(X, \mathbf{D})$  part of the system. Thus the resultant state  $\rho_{OZXE}$  of the executing protocol  $\Pi$  admits the following decomposition:

$$\rho_{OZXE} = \Psi_\Pi \otimes \text{id}_E(\rho_{X\mathbf{D}E}) = |\text{Acc}\rangle \otimes \rho_{ZXE}^{\text{Acc}} + |\text{Rej}\rangle \otimes \rho_{ZXE}^{\text{Rej}},$$

where  $\rho_{ZXE}^{\text{Acc}}, \rho_{ZXE}^{\text{Rej}}$  are sub-normalized states. For randomness amplification and certification protocols, we are interested in whether  $Z$  is close to uniform when the protocol accepts. (i.e., in the “accepting” state  $\rho_{ZXE}^{\text{Acc}}$ ). To that end, we define the following “ideal” super-operator (denoted  $\Phi_{\text{ideal}}(\cdot)$ ), and study the distance between  $\rho_{OZXE}$  and  $\Phi_{\text{ideal}}^Z(\rho_{OZXE})$ . Informally,  $\Phi_{\text{ideal}}(\cdot)$  replaces  $Z$  by an independent uniform string when  $O = \text{Acc}$  and leave the state untouched when  $O = \text{Rej}$ .

**Definition 4.1** The “ideal” super-operator  $\Phi_{\text{ideal}}^Z(\cdot)$  over  $\mathcal{L}(O \otimes \mathcal{Z} \otimes \mathcal{X} \otimes \mathcal{E})$  is defined as

$$\Phi_{\text{ideal}}^Z(\cdot) \stackrel{\text{def}}{=} |\text{Acc}\rangle (\langle \text{Acc}| \cdot |\text{Acc}\rangle) \otimes \Phi_{\text{unif}}^Z(\cdot) \otimes \text{id}_{\mathcal{X}\mathcal{E}}(\cdot) + |\text{Rej}\rangle (\langle \text{Rej}| \cdot |\text{Rej}\rangle) \otimes \text{id}_{\mathcal{Z}\mathcal{X}\mathcal{E}}(\cdot), \quad (4.1)$$

where  $\Phi_{\text{unif}}^Z(\cdot)$  is the “uniform” super-operator defined in Definition 3.4. For any protocol  $\Pi$  applied on  $\rho_{X\mathbf{D}E}$ , we define the distance  $\Delta(\Pi, \rho_{X\mathbf{D}E})$  as

$$\begin{aligned} \Delta(\Pi, \rho_{X\mathbf{D}E}) &\stackrel{\text{def}}{=} \left\| \Phi_\Pi \otimes \text{id}_E(\rho_{X\mathbf{D}E}) - \Phi_{\text{ideal}}^Z(\Phi_\Pi \otimes \text{id}_E(\rho_{X\mathbf{D}E})) \right\|_{\text{tr}} \\ &= \left\| \rho_{OZXE} - \Phi_{\text{ideal}}^Z(\rho_{OZXE}) \right\|_{\text{tr}} = \left\| \rho_{ZXE}^{\text{Acc}} - \Phi_{\text{unif}}^Z(\rho_{ZXE}^{\text{Acc}}) \right\|_{\text{tr}}. \end{aligned}$$

## 4.1 Randomness Amplification Protocol

We proceed to define randomness amplification protocols, which is the main object studied in this paper. Intuitively, the goal of a randomness amplification protocol is to generate certified uniform randomness from any weak source with sufficient entropy and untrusted devices, and should satisfy the following two properties: (i) (completeness) when the devices are “*honest*” (i.e., following the prescribed design) and the source has sufficient entropy, the protocol should accept with high probability and the output should be close to uniformly random, and (ii) (soundness) when the devices are *malicious*, the protocol should either reject with high probability, or still guarantee that the output is close to uniform when the protocol accepts. The following definition captures both properties concisely.

**Definition 4.2** *A protocol  $\Pi$  is a randomness amplification protocol for  $(n, k)$ -source with completeness error  $\epsilon_c$  and soundness error  $\epsilon_s$  if it satisfies the following completeness and soundness properties.*

**Completeness** *There exists a quantum-admissible strategy for devices  $\mathbf{D}$  such that for every source  $X$*

$$\Pr[\Pi(X, \mathbf{D}) \text{ accepts}] \geq 1 - \epsilon_c. \quad (4.2)$$

**Soundness** *For every joint system  $\rho_{X\mathbf{D}E}$  of the source, devices and the environment such that  $H_\infty(X|\mathbf{D}) \geq k$ , and let  $\rho_{OZXE} = \Phi_\Pi \otimes \text{id}_E(\rho_{X\mathbf{D}E})$ , then we have*

$$\Delta(\Pi, \rho_{X\mathbf{D}E}) = \|\rho_{OZXE} - \Phi_{\text{ideal}}^Z(\rho_{OZXE})\|_{\text{tr}} \leq \epsilon_s. \quad (4.3)$$

We illustrate the above definition with the following discussion.

- For completeness, one may note that it does not explicitly require the output  $Z$  to be close to uniform, but only requires the protocol to accept with high probability when operates on “honest” devices. Nevertheless, note that this is implied by combining both completeness and soundness properties. Indeed, when both (4.2) and (4.3) hold,  $(Z|\text{Acc}, X, E)$  is  $(\epsilon_c + \epsilon_s)$ -close to uniform in trace distance.
- For soundness, we formulate it by measuring the trace distance between the output state with its “idealized” version, which is also used before in, e.g., [GMdlT<sup>+</sup>12]. An alternative formulation is to require that either  $\Pr[\Pi(X, \mathbf{D}) \text{ accepts}] \leq \epsilon$  or  $(Z|\text{Acc}, X, E)$  is  $\epsilon$ -close to uniform, which is used in, e.g., [VV12a, VV12b]. The two formulations are equivalent up to certain parameter loss. For example, (4.3) implies that the alternative formulation with  $\epsilon = \sqrt{\epsilon_s}$ .
- We remark that in the definition of the source, we only require the source  $X$  to have  $k$  bits of min-entropy conditioned on the devices  $\mathbf{D}$ , as opposite to both  $\mathbf{D}$  and the environment  $E$ , which makes the definition stronger. This is also significant in our eyes since one may have better confidence on the amount of entropy in  $X$  with respect to bounded-size devices  $\mathbf{D}$  than with respect to the environment  $E$  that meant to capture the rest of the universe.
- We also remark that both our completeness and soundness definitions provide stronger guarantee than what are intuitively required in some aspects. For completeness, we require  $\Pi(X, \mathbf{D})$  to accept with high probability for *every* source  $X$  (instead of only for high min-entropy sources). For soundness, we require the output  $Z$  to be close to uniform even conditioned on the source



$X$  (not just the environment  $E$ ). We choose to provide stronger definitions since our protocol can achieve them and that stronger properties may be useful for additional applications.<sup>6</sup>

- We remark that our choice of  $H_\infty(X|\mathbf{D})$  can be extended easily to the smooth min-entropy  $H_\infty^{\epsilon_m}(X|\mathbf{D})$  by allowing an extra error  $\epsilon_m$  in soundness error.

**Desired Properties.** We briefly articulate desired properties for a randomness amplification protocol  $\Pi$ . Naturally, we would like to investigate small amount of min-entropy  $k$  to generate long and high-quality certified randomness (measured by output length  $\ell$  and soundness error  $\epsilon_s$ ) efficiently, where the efficiency can be measured by the number of devices  $t$  and the query and time complexity of  $\Pi$ . Note that since the devices can generate randomness, one can hope that the output length  $\ell$  is larger than the investigated entropy  $k$ ; that is, to achieve *expansion* property. We also note that high quality randomness is essential for some applications such as cryptography, and it is desirable to have soundness error to be poly-logarithmic in the investigated entropy  $k$  and the complexity of  $\Pi$ .

More importantly, for it to be possible to empirically perform the protocol in labs, *robustness* is essential, which is a strengthening of completeness that requires the protocol to accept with high probability even when a small constant amount of noise is presented in the honest devices (as noise is unavoidable in real-life). Note that formalizing the robustness property requires to specify the noise model, but there appears no “universal” error model that captures reality, and arguably the right error model may depend on the actual construction of the protocol and the honest devices. Therefore, we choose not to formalize the robust property as part of our model definition, and instead discuss the robustness property of constructed protocols.

## 4.2 Randomness Certification Protocol

Towards construction of randomness amplification protocol, we consider a significantly weaker task of randomness certification, where the goal is to certify uniform randomness produced by the devices (against the environment) using a *uniform* seed.

**Definition 4.3** *A protocol  $\Pi$  is a randomness certification protocol with seed length  $n$ , completeness error  $\epsilon_c$  and soundness error  $\epsilon_s$  if it satisfies the following completeness and soundness properties.*

**Completeness** *There exists a quantum-admissible strategy for devices  $\mathbf{D}$  such that for every source  $X$  (not necessarily uniform),*

$$\Pr[\Pi(X, \mathbf{D}) \text{ accepts}] \geq 1 - \epsilon_c$$

**Soundness** *For every joint system  $\rho_{X\mathbf{D}E}$  of the source, devices and the environment such that  $\rho_{X\mathbf{D}E} = \mathcal{U}_X \otimes \rho_{\mathbf{D}E}$ , and let  $\rho_{OZXE} = \Phi_\Pi \otimes \text{id}_E(\rho_{X\mathbf{D}E})$ , then we have*

$$\Delta(\Pi, \rho_{X\mathbf{D}E}) = \|\rho_{OZXE} - \Phi_{\text{ideal}}^Z(\rho_{OZXE})\|_{\text{tr}} \leq \epsilon_s.$$

The task of certifying randomness using truly random seeds has been investigated before in contexts such as quantum-secure device independent randomness expansion (DI-RE) and key distribution (DI-QKD), but with *additional* requirements. For randomness expansion, it additionally requires the

---

<sup>6</sup>For example, our construction of randomness amplification protocols crucially relies the corresponding stronger properties of randomness certification protocols (and inherits these properties).

expansion property that the certified randomness is longer than the original seed. For DI-QKD, the certification needs to be done between two separated parties where the adversarial eavesdropper gets to see the message exchanges of both parties.

In contrast, here we merely require that the output is close to uniform against the environment when given the seed  $X$  (so that the entropy must come from the devices and avoid the trivial solution of simply outputting the seed) and we are happy with certifying just a single bit using a long seed, which a-priori may look uninteresting. Interestingly, we will show that this is already sufficient to construct randomness amplification protocols.

Note that as in the definition of randomness amplification protocols, we require completeness to hold for *every* distribution  $X$  and the output is uniform *even* conditioned on the seed  $X$ . These properties are crucial for us to construct randomness amplification protocols using randomness certification protocols (and the constructed protocol inherits these properties). Nevertheless, known quantum-secure DI-RE and DI-QKD protocols of Vazirani and Vidick [VV12a, VV12b] satisfy the above definition.<sup>7</sup> Additionally, in a very recent result, Miller and Shi [MS13] present a novel randomness certification protocol that is *robust* and can certify *arbitrarily long* uniform randomness.

**Theorem 4.4** ([MS13]) *For every  $n, \ell \in \mathbb{N}$ , there exists a randomness certification protocol with seed length  $n$ , completeness and soundness error  $2^{-O(\sqrt{n})}$ , and output length  $\ell$ . Additionally, the protocol can tolerate  $\Omega(1)$  noise rate (in the sense that the protocol proceeds in “rounds”, and the devices’ output for each round of query may be changed with  $\Omega(1)$  chance), uses  $O(\log^* \ell)$  devices, and is efficient in the sense that it runs in time  $\text{poly}(n, \ell)$ .*

**Strong Randomness Certification.** Our construction of randomness amplification protocols relies on a (seemingly) stronger variant of randomness certification protocols.

**Definition 4.5** *A protocol  $\Pi$  is a strong randomness certification protocol with seed length  $n$ , completeness error  $\epsilon_c$  and soundness error  $\epsilon_s$  if it satisfies the completeness in Definition 4.3 and the following strong soundness properties.*

**Strong Soundness** *For every joint system  $\rho_{XDE}$  of the source, devices and environment such that  $\rho_{XD} = \mathcal{U}_X \otimes \rho_D$ , while  $X$  can be correlated with  $\mathcal{E}$  system, and let  $\rho_{OZXE} = \Phi_\Pi \otimes \text{id}_\mathcal{E}(\rho_{XDE})$ , then we have*

$$\Delta(\Pi, \rho_{XDE}) = \|\rho_{OZXE} - \Phi_{\text{ideal}}^Z(\rho_{OZXE})\|_{\text{tr}} \leq \epsilon_s.$$

The difference between *strong* and *regular* soundness is in the condition of soundness—regular soundness assumes that the seed  $X$  is uniform and independent of both the devices and the environment, whereas strong soundness only assumes that the seed  $X$  looks uniform from the devices. However, as we show in Lemma 4.6, regular soundness implies strong soundness and hence the two soundness notions are equivalent.

Intuitively, the lemma says that to certify randomness produced by  $\mathbf{D}$  with respect to  $E$ , it suffices to require the seed  $X$  to be looked random for the devices. While the statement may look quite intuitive, we emphasize that it may not be true in variant settings and here we crucially rely on that

---

<sup>7</sup>Specifically, the protocol of [VV12a] with seed length  $n$  certifies sub-exponential number  $\ell = 2^{n^\epsilon}$  of bits of uniform randomness with exponentially small completeness error and soundness error  $1/\text{poly}(\ell)$ , but is not robust. The protocol of [VV12b] is robust but only certifies  $\Omega(n)$  bits of uniform randomness with exponentially small completeness and soundness error.

- (i) we consider device-independent setting (i.e., the devices are prepared by the environment), and
- (ii) we consider stronger soundness guarantee that the output is close to uniform even conditioned on both the source  $X$  and the environment  $E$ .

**Lemma 4.6** *Every randomness certification protocol  $\Pi$  is also a strong randomness certification protocol with the same set of parameters.*

**Proof.** By definition, every randomness certification protocol  $\Pi$  satisfies the completeness of strong randomness certification protocols. It suffices to show that regular soundness shall imply strong soundness. Imagine any initial state  $\xi_{XDE}$  that only satisfies  $\xi_{XD} = \mathcal{U}_X \otimes \xi_D$ . We could represent  $\xi_{XDE}$  as follows

$$\xi_{XDE} = \sum_x \frac{1}{\dim(\mathcal{X})} |x\rangle\langle x| \otimes |\psi^x\rangle\langle\psi^x|_{DE},$$

in which without loss of generality we assume the for any given  $x$ , the quantum state of  $(D, E)$  is a pure state<sup>8</sup>. Moreover, we have  $\text{tr}_{\mathcal{E}}(|\psi^x\rangle\langle\psi^x|_{DE}) = \xi_D$  for every  $x$ . Let  $|\psi^0\rangle_{DE} \in \text{Dens}(D \otimes \mathcal{E})$  be any purification of  $\xi_D$ . By unitary equivalence of purifications, there exists a unitary operation  $U_E^x$  on  $\mathcal{E}$  system such that

$$|\psi^x\rangle_{DE} = (\text{id}_D \otimes U_E^x) |\psi^0\rangle_{DE}. \quad (4.4)$$

Let  $U_T$  be the controlled- $U_E^x$  operation over  $\mathcal{X} \otimes \mathcal{E}$  such that

$$U_T = \sum_x |x\rangle\langle x| \otimes U_E^x,$$

whose corresponding super-operator is denoted by  $\Phi_T$ . Let  $\rho_{XDE} = \Phi_T \otimes \text{id}_D(\xi_{XDE})$  and it follows from (4.4) that

$$\rho_{XDE} = \mathcal{U}_X \otimes |\psi^0\rangle\langle\psi^0|_{DE}. \quad (4.5)$$

Our proof then follows from two observations. The first one is that by soundness of protocol  $\Pi$  and (4.5), we have

$$\Delta(\Pi, \rho_{XDE}) = \|\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\rho_{XDE}) - \Phi_{\text{ideal}}^Z(\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\rho_{XDE}))\|_{\text{tr}} \leq \epsilon_s.$$

Moreover, one could observe that  $\Phi_T$  and  $\Phi_{\Pi}$ , or  $\Phi_{\text{ideal}}^Z$ , commute with each other. For  $\Phi_T$  and  $\Phi_{\Pi}$ , this is because the common space  $\mathcal{X}$  they apply on is classical and both  $\Phi_T$  and  $\Phi_{\Pi}$  leave  $\mathcal{X}$  unchanged. For  $\Phi_T$  and  $\Phi_{\text{ideal}}^Z$ , this is because they apply on disjoint systems, i.e.,  $\Phi_T$  applies on  $\mathcal{X} \otimes \mathcal{E}$  and  $\Phi_{\text{ideal}}^Z$  only non-trivially applies on  $O \otimes \mathcal{Z}$ . Thus, by noting that  $\rho_{XDE} = \Phi_T \otimes \text{id}_D(\xi_{XDE})$ , we have

$$\begin{aligned} \Delta(\Pi, \rho_{XDE}) &= \|\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\Phi_T \otimes \text{id}_D(\xi_{XDE})) - \Phi_{\text{ideal}}^Z(\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\Phi_T \otimes \text{id}_D(\xi_{XDE})))\|_{\text{tr}} \\ &= \|\Phi_T \otimes \text{id}_D(\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\xi_{XDE})) - \Phi_{\text{ideal}}^Z(\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\xi_{XDE}))\|_{\text{tr}} \\ &= \|\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\xi_{XDE}) - \Phi_{\text{ideal}}^Z(\Phi_{\Pi} \otimes \text{id}_{\mathcal{E}}(\xi_{XDE}))\|_{\text{tr}} = \Delta(\Pi, \xi_{XDE}), \end{aligned}$$

where the second equality is because of the commutation between  $\Phi_T$  and  $\Phi_{\Pi}$ , and between  $\Phi_T$  and  $\Phi_{\text{ideal}}^Z$ . The last equality is because  $\Phi_T$  is a unitary operation and thus does not change the trace norm. Thus we have  $\Delta(\Pi, \xi_{XDE}) \leq \epsilon_s$ , which shows the protocol  $\Pi$  also has strong soundness.  $\blacksquare$

---

<sup>8</sup>This is because the state  $|\psi^x\rangle$  is prepared by the environment and holding pure states can only increase its power to cheat.

## 5 Quantum Somewhere Random Source

In this section, we introduce quantum analogue of somewhere random sources, which is the main conceptual object in our construction. In classical setting, a somewhere random source  $\mathbf{S}$  is simply a sequence of random variables  $\mathbf{S} = (S_1, \dots, S_t)$  such that the marginal distribution of some block  $S_i$  is uniform (but there could be arbitrary correlation among them). Somewhere random sources are useful intermediate objects for several constructions of randomness extractors (see, e.g., [Rao07, Li13]), but to the best of our knowledge, its quantum analogue has not been considered before. We provide a quantum analogue definition by explicitly modelling the quantum correlation (as was done in the literature of quantum-proof randomness extractor).

**Definition 5.1 (Quantum-SR Source)** *A cq-state  $\rho \in \text{Dens}(S_1 \otimes \dots \otimes S_t \otimes E)$  with classical part  $S_1, S_2, \dots, S_t \in \{0, 1\}^m$  and quantum part  $E$  is a  $(t, m)$ -quantum somewhere random source against  $E$  if there exists  $i \in [t]$  such that*

$$\rho_{S_i E} = \mathcal{U}_m \otimes \rho_E,$$

where  $\rho_{S_i E}$  and  $\rho_E$  are reduced states of  $\rho$  on  $S_i \otimes \mathcal{E}$  and  $\mathcal{E}$  systems respectively. We say  $\rho$  is a  $(t, m, \epsilon)$ -quantum somewhere random source if there exists  $i \in [t]$  such that

$$\frac{1}{2} \|\rho_{S_i E} - \mathcal{U}_m \otimes \rho_E\|_{\text{tr}} \leq \epsilon.$$

We remark that the fact that  $\rho$  is a  $(t, m, \epsilon)$ -quantum somewhere random source does not necessarily imply that  $\rho$  is  $\epsilon$ -close in trace distance to some  $(t, m)$ -quantum somewhere random source  $\rho'$  (in contrast, the analogous statement is true for classical somewhere random source). On the other hand, just like its classical counterpart, one can convert a weak source  $X$  to a somewhere random source by applying a (quantum-proof) strong randomness extractor to  $X$  with all possible seeds (each seed yields one block).

**Definition 5.2 (Quantum-proof Strong Randomness Extractor)** *A function  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  is a quantum-proof (or simply quantum)  $(k, \epsilon)$ -strong randomness extractor, if for all states  $\rho_{XE}$  classical on  $X$  with  $H_\infty(X|E) \geq k$ , and for a uniform seed  $Y$  independent of  $\rho_{XE}$ , we have*

$$\frac{1}{2} \|\rho_{\text{Ext}(X, Y) Y E} - \mathcal{U}_m \otimes \rho_Y \otimes \rho_E\|_{\text{tr}} \leq \epsilon. \quad (5.1)$$

**Proposition 5.3** *Let  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a quantum-proof  $(k, \epsilon)$ -strong extractor. Let  $\rho_{XE}$  be a cq-state with  $H_\infty(X|E) \geq k$ . For every  $i \in \{0, 1\}^n$ , let  $S_i = \text{Ext}(X, i)$ . Then the cq-state*

$$\rho_{S_1 \dots S_{2^d} E} \stackrel{\text{def}}{=} \sum_x p_x |S_1\rangle\langle S_1| \otimes \dots \otimes |S_{2^d}\rangle\langle S_{2^d}| \otimes \rho_E^x,$$

is a  $(2^d, m, \epsilon)$ -quantum SR source.

**Proof.** Since  $\text{Ext}$  is a quantum-proof  $(k, \epsilon)$ -strong extractor and  $H_\infty(X|E) \geq k$ , we have that

$$\frac{1}{2} \|\rho_{\text{Ext}(X, Y) Y E} - \mathcal{U}_m \otimes \rho_Y \otimes \rho_E\|_{\text{tr}} \leq \epsilon,$$

which is equivalent to

$$\frac{1}{2} \sum_{i=1}^{2^d} \frac{1}{2^d} \left\| \rho_{\text{Ext}(X,i)E} - \mathcal{U}_m \otimes \rho_E \right\|_{\text{tr}} \leq \epsilon.$$

Thus immediately we have that there exists an index  $i \in [2^d]$  such that

$$\frac{1}{2} \left\| \rho_{\text{Ext}(X,s_i)E} - \mathcal{U}_m \otimes \rho_E \right\|_{\text{tr}} \leq \epsilon,$$

or equivalently  $\frac{1}{2} \left\| \rho_{S_i E} - \mathcal{U}_m \otimes \rho_E \right\|_{\text{tr}} \leq \epsilon$ . ■

We state the following two quantum strong randomness extractors in [DPVR12] that will be useful for us to instantiate our randomness amplification protocols.

**Theorem 5.4 ([DPVR12], Corollary 5.4)** *For every  $n, k \in \mathbb{N}$  and  $\epsilon > 0$  with  $k \geq 4 \log(1/\epsilon) + O(1)$ , there exists a quantum  $(k, \epsilon)$ -strong randomness extractor  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  with  $m = k - 4 \log(1/\epsilon) - O(1)$  and  $d = O(\log^2(n/\epsilon) \log m)$ .*

**Theorem 5.5 ([DPVR12], Corollary 5.6)** *Let  $0 < \gamma < \alpha < 1$  and  $a > 0$  be constants. For sufficiently large  $n$ , there exists a quantum  $(k, \epsilon)$ -strong randomness extractor  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  with,  $k = n^\alpha$  and  $\epsilon = n^{-a}$ ,  $m = O(n^{\alpha-\gamma})$ , and  $d = O\left(\frac{(1+a)^2}{\gamma} \log n\right)$ .*

## 6 Main Randomness Amplification Protocol

In this section, we construct our main randomness amplification protocol  $\Pi_{\text{amp}}$  based on any quantum-proof strong randomness extractor  $\text{Ext}$  and strong randomness certification protocol  $\Pi_{\text{cert}}$ .

Our construction is very simple: on input a weak source  $X$ ,  $\Pi_{\text{amp}}$  first uses the extractor  $\text{Ext}$  to turn  $X$  into a somewhere random source  $(S_1, \dots, S_{2^d})$  where  $d$  is the seed length of  $\text{Ext}$  and  $S_i = \text{Ext}(X, i)$ , and then for each  $i \in [2^d]$ , invokes the randomness certification protocol  $\Pi_{\text{cert}}$  with seed  $S_i$  and *distinct* set of devices  $\mathbf{D}_i$ , each of which outputs  $(O_i, Z_i)$ . If any of them rejects, then  $\Pi_{\text{amp}}$  reject; otherwise,  $\Pi_{\text{amp}}$  accepts and outputs  $Z = \bigoplus_{i \in [2^d]} Z_i$ . A formal description of the protocol can be found in Figure 3.

At a high level,  $\Pi_{\text{amp}}$  works because some block  $S_{i^*}$  will be close to uniform and thus can be used as the seed in  $\Pi_{\text{cert}}$  to certify that the output  $Z_{i^*}$  is close to uniform *even conditioned on everything except  $\mathbf{D}_{i^*}$* , which includes source  $X$ , environment  $E$ , the devices  $\mathbf{D}_{-i^*}$  used by other blocks (since we can view all of them as the environment for  $\Pi_{\text{cert}}$ ). This implies that  $Z_{i^*}$  is close to uniform conditioned on the outputs  $Z_{-i^*}$  of other blocks, and thus  $Z = Z_{i^*} \oplus \left(\bigoplus_{j \neq i^*} Z_j\right)$  is close to uniform. Formally, we prove the following main theorem.

**Theorem 6.1 (Main)** *If  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  is a quantum  $(k, \epsilon)$ -strong randomness extractor and  $\Pi_{\text{cert}}$  is a strong randomness certification protocol with seed length  $m$ , completeness error  $\epsilon_c$ , and soundness error  $\epsilon_s$ , then  $\Pi_{\text{amp}}$  is a randomness amplification protocol for  $(n, k)$ -source with completeness error  $2^d \cdot \epsilon_c$  and soundness error  $\epsilon_s + 4\sqrt{2\epsilon}$ .*

**Proof.** Let us prove  $\Pi_{\text{amp}}$ 's completeness first. By the completeness of  $\Pi_{\text{cert}}$ , there exists a quantum-admissible strategy for each device  $\mathbf{D}_i$  such that for every source  $S_i$  we have

$$\Pr[\Pi_{\text{cert}}(S_i, \mathbf{D}_i) \text{ accepts}] \geq 1 - \epsilon_c.$$

---

**Protocol  $\Pi_{\text{amp}}$**

---

Let  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a quantum-proof strong randomness extractor.

Let  $\Pi_{\text{cert}}$  be a randomness certification protocol with seed length  $m$  that uses  $t_{\text{cert}}$  devices.

$\Pi_{\text{amp}}$  operates on an input source  $X$  over  $\{0, 1\}^n$  and  $t_{\text{amp}} = 2^d \cdot t_{\text{cert}}$  devices  $\mathbf{D} = (\mathbf{D}_1, \dots, \mathbf{D}_{2^d})$ , where each  $\mathbf{D}_i$  denotes a set of  $t_{\text{cert}}$  devices, as follows.

1. For every  $i \in \{0, 1\}^d$ , let  $S_i = \text{Ext}(X, i)$  and invoke  $(O_i, Z_i) \leftarrow \Pi_{\text{cert}}(S_i, \mathbf{D}_i)$ .
  2. If there exists some  $O_i = \text{Rej}$ , then  $\Pi_{\text{amp}}$  outputs  $O = \text{Rej}$ ; otherwise,  $\Pi_{\text{amp}}$  outputs  $(O, Z) = (\text{Acc}, \bigoplus_{i \in [2^d]} Z_i)$ .
- 

Figure 3: Our Main Randomness Amplification Protocol  $\Pi_{\text{amp}}$ .

By the design of  $\Pi_{\text{amp}}$ , it accepts if every  $\Pi_{\text{cert}}(S_i, \mathbf{D}_i)$  accepts for  $i \in \{0, 1\}^d$ . Thus by the union bound, we have for this strategy,

$$\Pr[\Pi_{\text{amp}}(X, \mathbf{D}_i) \text{ accepts}] \geq 1 - 2^d \epsilon_c.$$

Thus, by definition,  $\Pi_{\text{amp}}$  has completeness error  $2^d \epsilon_c$ .

Let us proceed to the soundness of  $\Pi_{\text{amp}}$ . Let  $\vec{S} = S_1 \dots S_{2^d}$  and  $\vec{\mathbf{D}} = \mathbf{D}_1 \dots \mathbf{D}_{2^d}$ . Consider any initial state  $\rho_{X\vec{\mathbf{D}}_E}$  such that  $H_\infty(X|\vec{\mathbf{D}}) \geq k$ . Let  $S_i = \text{Ext}(x, i)$  for  $i \in \{0, 1\}^d$ . Thus by Proposition 5.3, we have that  $\rho_{\vec{S}\vec{\mathbf{D}}}$  is a  $(2^d, m, \epsilon)$ -quantum SR source. Hence, there exists an  $i^* \in \{0, 1\}^d$ , such that

$$\frac{1}{2} \|\rho_{S_{i^*}\mathbf{D}_{i^*}} - \mathcal{U}_{S_{i^*}} \otimes \rho_{\mathbf{D}_{i^*}}\|_{\text{tr}} \leq \epsilon. \quad (6.1)$$

Thus by Lemma 3.2, there exists a state  $\xi_{\vec{S}\vec{\mathbf{D}}_{XE}}$  such that  $\xi_{S_{i^*}\mathbf{D}_{i^*}} = \mathcal{U}_{S_{i^*}} \otimes \rho_{\mathbf{D}_{i^*}}$  (thus,  $\xi_{\mathbf{D}_{i^*}} = \rho_{\mathbf{D}_{i^*}}$  and  $\xi_{S_{i^*}\mathbf{D}_{i^*}} = \mathcal{U}_{S_{i^*}} \otimes \xi_{\mathbf{D}_{i^*}}$ ) such that

$$F(\rho_{S_{i^*}\mathbf{D}_{i^*}}, \xi_{S_{i^*}\mathbf{D}_{i^*}}) = F(\rho_{\vec{S}\vec{\mathbf{D}}_{XE}}, \xi_{\vec{S}\vec{\mathbf{D}}_{XE}}). \quad (6.2)$$

Then by Lemma 3.1 together with (6.1) (6.2), one obtains that

$$\frac{1}{2} \|\rho_{X\vec{\mathbf{D}}_E} - \xi_{X\vec{\mathbf{D}}_E}\|_{\text{tr}} \leq \frac{1}{2} \|\rho_{\vec{S}\vec{\mathbf{D}}_{XE}} - \xi_{\vec{S}\vec{\mathbf{D}}_{XE}}\|_{\text{tr}} \leq \sqrt{2\epsilon}.$$

By definition, we have  $\Delta(\Pi_{\text{amp}}, \rho_{X\vec{\mathbf{D}}_E}) = \|\Xi(\rho_{X\vec{\mathbf{D}}_E})\|_{\text{tr}}$ , where  $\Xi^0(\cdot) \stackrel{\text{def}}{=} \Phi_{\Pi_{\text{amp}}} \otimes \text{id}_{\mathcal{E}}(\cdot)$ ,  $\Xi^1(\cdot) \stackrel{\text{def}}{=} \Phi_{\text{ideal}}^Z(\Xi^0(\cdot))$ , and  $\Xi(\cdot) = \Xi^0(\cdot) - \Xi^1(\cdot)$ . Note that  $\Xi^0, \Xi^1$  are admissible super-operators. Let  $\tau = \rho_{X\vec{\mathbf{D}}_E} - \xi_{X\vec{\mathbf{D}}_E}$ . Thus, by triangle inequalities,

$$\Delta(\Pi_{\text{amp}}, \rho_{X\vec{\mathbf{D}}_E}) \leq \Delta(\Pi_{\text{amp}}, \xi_{X\vec{\mathbf{D}}_E}) + \Delta(\Pi_{\text{amp}}, \tau). \quad (6.3)$$

Moreover, by triangle inequalities and Fact 3.3, we have

$$\Delta(\Pi_{\text{amp}}, \tau) = \|\Xi(\tau)\|_{\text{tr}} \leq \|\Xi^0(\tau)\|_{\text{tr}} + \|\Xi^1(\tau)\|_{\text{tr}} \leq 2\|\tau\|_{\text{tr}} \leq 4\sqrt{2\epsilon}. \quad (6.4)$$

It then suffices to upper bound  $\Delta(\Pi_{\text{amp}}, \xi_{X\vec{\mathbf{D}}E})$ . To that end, we make a crucial use of the *strong soundness* of protocol  $\Pi_{\text{cert}}$  and study the *compositions* of  $\Pi_{\text{cert}}$  in  $\Pi_{\text{amp}}$ .

Let  $\Phi_{\Pi_{\text{cert}}}^{i^*}$  denote the super-operator of the  $i^*$ th  $\Pi_{\text{cert}}$  protocol. Note that  $\xi_{S_{i^*}\mathbf{D}_{i^*}} = \mathcal{U}_{S_{i^*}} \otimes \xi_{\mathbf{D}_{i^*}}$ , while  $S_{i^*}$  might be correlated with the environment  $E' = (S_{-i^*}, \mathbf{D}_{-i^*}, X, E)$ . Let  $\xi_{O_{i^*}Z_{i^*}S_{i^*}E'} = \Phi_{\Pi_{\text{cert}}}^{i^*} \otimes \text{id}_{\mathcal{E}'}(\xi_{S_{i^*}\mathbf{D}_{i^*}E'})$  that admits the following decomposition:

$$|\text{Acc}\rangle \otimes \xi_{Z_{i^*}S_{i^*}E'}^{\text{Acc}} + |\text{Rej}\rangle \otimes \xi_{Z_{i^*}S_{i^*}E'}^{\text{Rej}}$$

Thus, by the strong soundness of  $\Pi_{\text{cert}}$ , we have

$$\Delta(\Pi_{\text{cert}}, \xi_{S_{i^*}\mathbf{D}_{i^*}E'}) = \left\| \xi_{Z_{i^*}S_{i^*}E'}^{\text{Acc}} - \mathcal{U}_{Z_{i^*}} \otimes \xi_{S_{i^*}E'}^{\text{Acc}} \right\|_{\text{tr}} \leq \epsilon_s. \quad (6.5)$$

Let  $\Phi^{-i^*}$  denote all other operations in  $\Pi_{\text{amp}}$  that are applied on the environment  $E'$ , including applying  $\Pi_{\text{cert}}$  to each  $(S_i, \mathbf{D}_i)$  such that  $i \neq i^*$ , and outputting  $O_{-i^*} = \text{Acc}$  iff  $\forall i \neq i^*, O_i = \text{Acc}$  as well as  $Z_{-i^*} = \bigoplus_{i \neq i^*} Z_i$ . Let  $E'' = (\vec{S}, X, E)$ . By definition, the resultant state  $\xi_{O_{i^*}Z_{i^*}O_{-i^*}Z_{-i^*}E''}$  is

$$|\text{Acc}, \text{Acc}\rangle \otimes \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Acc}, \text{Acc}} + |\text{Acc}, \text{Rej}\rangle \otimes \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Acc}, \text{Rej}} + |\text{Rej}, \text{Acc}\rangle \otimes \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Rej}, \text{Acc}} + |\text{Rej}, \text{Rej}\rangle \otimes \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Rej}, \text{Rej}}.$$

One could also apply  $\Phi^{-i^*}$  to both  $\xi_{Z_{i^*}S_{i^*}E'}^{\text{Acc}}$  and  $\mathcal{U}_{Z_{i^*}} \otimes \xi_{S_{i^*}E'}^{\text{Acc}}$  in (6.5). Given Fact 3.3, together with the fact  $O_{-i^*}$  being classical, we have

$$\left\| \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Acc}, \text{Acc}} - \mathcal{U}_{Z_{i^*}} \otimes \xi_{Z_{-i^*}E''}^{\text{Acc}, \text{Acc}} \right\|_{\text{tr}} \leq \epsilon_s. \quad (6.6)$$

The last step is to output the final decision  $O = \text{Acc}$  iff  $O_{i^*} = O_{-i^*} = \text{Acc}$  and  $Z = Z_{i^*} \oplus Z_{-i^*}$ . Namely, we arrive at the following state

$$|\text{Acc}\rangle \otimes \xi_{ZE''}^{\text{Acc}, \text{Acc}} + |\text{Rej}\rangle \otimes (\xi_{ZE''}^{\text{Acc}, \text{Rej}} + \xi_{ZE''}^{\text{Rej}, \text{Acc}} + \xi_{ZE''}^{\text{Rej}, \text{Rej}}).$$

Let  $\Phi_{\text{XOR}} : \mathcal{L}(Z_1 \otimes Z_2) \rightarrow \mathcal{L}(Z)$  be the operation that outputs  $Z = Z_1 \oplus Z_2$  of inputs  $Z_1, Z_2$ . By definition, we have

$$\Phi_{\text{XOR}} \otimes \text{id}_{\mathcal{E}''}(\xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Acc}, \text{Acc}}) = \xi_{ZE''}^{\text{Acc}, \text{Acc}}.$$

By Lemma 6.2, we have

$$\Phi_{\text{XOR}} \otimes \text{id}_{\mathcal{E}''}(\mathcal{U}_{Z_{i^*}} \otimes \xi_{Z_{-i^*}E''}^{\text{Acc}, \text{Acc}}) = \mathcal{U}_Z \otimes \xi_{E''}^{\text{Acc}, \text{Acc}}.$$

Therefore, by definition of  $\Delta(\Pi_{\text{amp}}, \xi_{X\vec{\mathbf{D}}E})$ , together with Fact 3.3 and (6.6), we have

$$\Delta(\Pi_{\text{amp}}, \xi_{X\vec{\mathbf{D}}E}) = \left\| \xi_{ZE''}^{\text{Acc}, \text{Acc}} - \mathcal{U}_Z \otimes \xi_{E''}^{\text{Acc}, \text{Acc}} \right\|_{\text{tr}} \leq \left\| \xi_{Z_{i^*}Z_{-i^*}E''}^{\text{Acc}, \text{Acc}} - \mathcal{U}_{Z_{i^*}} \otimes \xi_{Z_{-i^*}E''}^{\text{Acc}, \text{Acc}} \right\|_{\text{tr}} \leq \epsilon_s. \quad (6.7)$$

Finally, by (6.3), (6.4) and (6.7), we have

$$\Delta(\Pi_{\text{amp}}, \rho_{X\vec{\mathbf{D}}E}) \leq \Delta(\Pi_{\text{amp}}, \xi_{X\vec{\mathbf{D}}E}) + 4\sqrt{2}\epsilon \leq \epsilon_s + 4\sqrt{2}\epsilon,$$

which, by definition, shows that  $\Pi_{\text{amp}}$  has soundness error  $\epsilon_s + 4\sqrt{2}\epsilon$ . ■

**Lemma 6.2** Let  $Z_1, Z_2 \in \{0, 1\}^t$  and  $\Phi_{\text{XOR}}$  denote the operation that takes  $Z_1, Z_2$  as inputs and output  $Z = Z_1 \oplus Z_2$ . Thus for any  $\rho_{Z_2E}$ , we have

$$\Phi_{\text{XOR}} \otimes \text{id}_{\mathcal{E}}(\mathcal{U}_{Z_1} \otimes \rho_{Z_2E}) = \mathcal{U}_Z \otimes \rho_E.$$

**Proof.** Observe that

$$\mathcal{U}_{Z_1} \otimes \rho_{Z_2 E} = \sum_{z_1, z_2} \frac{1}{2^t} p_{z_2} |z_1, z_2\rangle \langle z_1, z_2| \otimes \rho_E^{z_2}.$$

Thus, it follows from easy calculation that

$$\Phi_{\text{XOR}} \otimes \text{id}_{\mathcal{E}}(\mathcal{U}_{Z_1} \otimes \rho_{Z_2 E}) = \sum_z \frac{1}{2^t} |z\rangle \langle z| \otimes \sum_{z_1 \oplus z_2 = z} p_{z_2} \rho_E^{z_2} = \mathcal{U}_Z \otimes \rho_E.$$

■

## 7 Instantiations of Our Main Protocol

In this section, we provide several instantiations of our randomness amplification protocol that optimize different parameters by plugging in appropriate quantum strong randomness extractors and randomness certification protocols.

Note that our main protocol inherits the output length and the robustness property from the randomness certification protocol, but pays a factor of  $2^d$  in the completeness error and the efficiency (in terms of the number of devices and time and query complexity of the protocol, where  $d$  is the seed length of the randomness extractor). By taking advantage of the Miller-Shi protocol [MS13] (Theorem 4.4), we can certify uniform randomness of an arbitrarily length. On the other hand, we plug in two extractors of De et al. [DPVR12] (Theorem 5.4 and 5.5) to optimize different parameters.

We first optimize over the quality of the certified randomness, namely, minimizing the soundness error. By plugging in the randomness extractor from Theorem 5.4 and the randomness certification protocol from Theorem 4.4, we obtain the following corollary.

**Corollary 7.1** *For every  $n, k, \ell \in \mathbb{N}$  and  $\epsilon \in (0, 1)$  such that  $k \geq O(\log^5 \frac{n}{\epsilon})$ , there exists a randomness amplification protocol for  $(n, k)$ -source with completeness error  $2^{-O(\sqrt{k})}$ , soundness error  $\epsilon$ , and output length  $\ell$ . Additionally, the protocol can tolerate  $\Omega(1)$  noise rate (in the same sense as Theorem 4.4). The protocol uses  $t = O(2^{O(\log^2(n/\epsilon) \cdot \log k)} \cdot \log^* \ell)$  devices and has runtime  $\text{poly}(t, \ell)$ .*

For sufficiently large  $k \geq \text{poly} \log(n)$ , Corollary 7.1 yields a *robust* protocol with *sub-exponentially* small soundness error  $\epsilon \leq 2^{-k^{\Omega(1)}}$  in the amount of min-entropy  $k$  in the source that certifies an *arbitrarily long* uniform randomness.

**Remark 7.2 (comparison with previous works of [GMdIT<sup>+</sup>12])** In comparison to the previous work of Gallego et al. [GMdIT<sup>+</sup>12], the above protocol has significant qualitative improvement in several aspects as well as quantitatively exponential improvements in several parameters. More precisely, Gallego et al. [GMdIT<sup>+</sup>12] constructs a randomness amplification protocol for Santa-Vazirani sources (as opposed to general weak sources) with inverse polynomial soundness error in the source length  $n$  that certifies only a single bit of randomness. Additionally, the protocol is not robust and due to the use of a non-constructive “deterministic hash function”, the protocol has exponential runtime in  $n$  and  $1/\epsilon$  (in order to search for the function by enumeration). Thus, our protocol has the qualitative improvement of handling general weak source, achieving robustness, and certifying arbitrarily long randomness, and quantitatively achieves exponentially small error and quasi-polynomial runtime in  $n$  and  $1/\epsilon$ .



We next focus on the efficiency and consider the natural requirement that the protocol runs in polynomial time in the source length  $n$ . By plugging in the randomness extractor from Theorem 5.4 and the randomness certification protocol from Theorem 4.4, we obtain the following corollary.

**Corollary 7.3** *Let  $0 < \gamma < \alpha < 1$  and  $a, c > 0$  be constants. For every sufficiently large  $n \in \mathbb{N}$ , there exists a randomness amplification protocol for  $(n, n^\alpha)$ -source with completeness error  $2^{-O(n^{\gamma/2})}$ , soundness error  $n^{-a}$ , and output length  $\ell = n^c$ . Additionally, the protocol can tolerate  $\Omega(1)$  noise rate (in the same sense as Theorem 4.4), uses  $\text{poly}(n)$  devices and has runtime  $\text{poly}(n)$ .*

In contrast to Corollary 7.1, the protocol in Corollary 7.3 has polynomial runtime but requires the source to have  $k = n^{\Omega(1)}$  bits of min-entropy and only achieves inverse polynomial soundness error. It is interesting to note that for cryptographic applications, high quality randomness (namely, negligibly close to uniform in the security parameter) is often necessary, but our Corollary 7.3 only achieves inverse polynomial error (unless the protocol has super-polynomial runtime, which is not reasonable). We thus leave the following as a major open question from our work that: Can “*cryptographic quality*” randomness amplification protocol be achieved?

Finally, we aim for optimizing robustness. While the protocol of Miller-Shi [MS13] tolerates a constant level of noise, the constant is not determined in their work. To obtain better robustness, one could instead rely on the randomness certification protocol of [VV12b] from the context of DI-QKD, which can tolerate roughly 1.2% noise. We here further optimize the robustness property by *directly* constructing a new strong randomness certification protocol that can tolerate roughly 1.748% noise, at the price that it only certifies one random bit with inverse polynomial soundness error (but still improve over previous result of Gallego et al [GMdIT<sup>+</sup>12] which additionally is not robust and only handles SV sources). We state our protocol in the following theorem, and defer its construction and analysis to Appendix B, and additional preliminaries to Appendix A.

**Theorem 7.4** *For every sufficiently large  $n \in \mathbb{N}$ , there exists a randomness certification protocol with seed length  $n$ , completeness error  $2^{-\Omega(n)}$ , soundness error  $O(n^{-\beta})$ , and output length 1, where  $\beta \in (0, 1)$  is a small universal constant. Additionally, the protocol can tolerate 1.748% noise rate (in the sense that the protocol proceeds in “rounds,” and the devices’ output for each round of query may be changed with  $\Omega(1)$  chance), uses  $\text{poly}(n)$  devices and has runtime  $\text{poly}(n)$ .*

Plugging in our randomness certification protocol with the randomness extractor from Theorem 5.5, we obtain the following corollary.

**Corollary 7.5** *Let  $0 < \gamma < \alpha < 1$  be constants. For every sufficiently large  $n \in \mathbb{N}$ , there exists a randomness amplification protocol for  $(n, n^\alpha)$ -source with completeness error  $2^{-O(n^\gamma)}$ , soundness error  $O(n^{-\beta})$ , and output length 1. Additionally, the protocol can tolerate 1.748% noise rate (in the same sense as Theorem 7.4), uses  $\text{poly}(n)$  devices and has runtime  $\text{poly}(n)$ .*

**Remark 7.6** Instead of invoking Lemma 4.6 to transform regular soundness to strong soundness, we *directly* prove the strong soundness of our protocol in Theorem 7.4 (or in Figure 4). In this sense, our analysis is stronger than those in [VV12a, VV12b, MS13] which needs Lemma 4.6 to achieve strong soundness. Our protocol is based on BHK games and makes crucial use of its strong monogamy phenomenon, which resembles the protocols of Gallego et al [GMdIT<sup>+</sup>12], though with simple bipartite non-local games. Another advantage of this protocol, similar to [GMdIT<sup>+</sup>12], is its *non-signaling* security, while the analysis of protocols in [VV12a, VV12b, MS13] vitally relies on assuming quantum mechanics.

## References

- [BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.
- [Blu86] Manuel Blum. Independent unbiased coin flips from a correlated biased source: a finite Markov chain. *Combinatorica*, 6(2):97–108, 1986.
- [CR12] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8:450–453, 2012.
- [DPVR12] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisans extractor in the presence of quantum side information. *SIAM Journal on Computing*, 067(258932), 2012.
- [GHH<sup>+</sup>13] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan. Free randomness amplification using bipartite chain correlations, 2013.
- [GMdIT<sup>+</sup>12] Rodrigo Gallego, Lluís Masanes, Gonzalo de la Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. Full randomness from arbitrarily deterministic events, October 24 2012. Comment: 4 pages, 2 figures + appendices.
- [JUW09] R. Jain, S. Upadhyay, and J. Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 534–543, 2009. arXiv:0905.1300v1 [quant-ph].
- [Li13] Xin Li. New independent source extractors with exponential improvement. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, 2013.
- [Mas09] Lluís Masanes. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.*, 102:140501, Apr 2009.
- [MP13] P. Mironowicz and M. Pawowski. Amplification of arbitrarily weak randomness, 2013.
- [MRC<sup>+</sup>06] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett. Unconditional security of key distribution from causality constraints, 2006.
- [MS13] Carl A. Miller and Yaoyun Shi. Self-testing quantum dice certified by a uncertainty principle. Personal communication, 2013.
- [Rao07] Anup Rao. *Randomness Extractors for Independent Sources and Applications*. PhD thesis, The University of Texas at Austin, 2007.
- [RBG<sup>+</sup>13] Ravishankar Ramanathan, Fernando GSL Brandao, Andrzej Grudka, Karol Horodecki, Michał Horodecki, and Paweł Horodecki. Robust device independent randomness amplification. 2013. arxiv:1308.4635.
- [Ren05] Renato Renner. Security of quantum key distribution, January 11 2005. Comment: PhD thesis; index added.
- [RWW06] Renato Renner, Stefan Wolf, and Juerg Wullschlegel. The single-serving channel capacity. August 02 2006. Comment: 4 pages, latex.

- [SV84] M. Santha and U. V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS 1984)*, page 434, 1984.
- [Vad07] Salil Vadhan. The unified theory of pseudorandomness. *SIGACT News*, 38(3):39–54, September 2007.
- [VV12a] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 370(1971):3432–3448, 2012.
- [VV12b] Umesh Vazirani and Thomas Vidick. Fully device independent quantum key distribution. arXiv:1210.1810v2, 2012.
- [Zuc90] D. Zuckerman. General weak random sources. In *Foundations of Computer Science, 1990. Proceedings., 31st Annual Symposium on*, pages 534–543 vol.2, 1990.

## A Additional Preliminaries for Protocol $\Pi_{\text{BHK}}$ in Fig. 4

**Non-signaling Strategies.** Let  $P_{AB|XY}$  denote a non-signaling (NS) strategy for any bi-partite nonlocal game, where  $X, Y$  are Alice and Bob’s inputs respectively, and  $A, B$  are Alice and Bob’s outputs respectively. Note that each entry  $P_{ab|xy}$  is the probability of outputting  $a$  and  $b$  given input  $x$  and  $y$ , where we adopt the convention that capital variables (e.g.,  $A, X$ ) denote random variables and small case variables (e.g.,  $a, x$ ) denote specific values of random variables, i.e.  $A = a, X = x$ . Let  $P_{A|X}$  denote Alice’s output  $A$ ’s distribution given input  $X$ . Similarly, one could define  $P_{B|Y}$  for Bob. The non-signaling condition requires that

$$\sum_b P_{Ab|Xy} = P_{A|X}, \forall y \quad \text{and} \quad \sum_a P_{aB|xY} = P_{B|Y}, \forall x.$$

One could also consider playing multiple copies of the same non-local game in parallel (i.e., on separate non-local boxes). In this case, we denote any NS-strategy for the whole game  $\mathbf{P}_{\mathbf{AB}|\mathbf{XY}}$ , in which we use **bold** font variables for multiple copies.

One can also consider the effect of a NS-strategy when conditioned on certain inputs and outputs of some parties. For example, let  $P_{ABF|XYE}$  be any three-partite (Alice, Bob, and Eve) NS-strategy and let Eve’s side input be  $e$  and output be  $f$ . Then one could define the conditional strategy (denoted  $P_{AB|XY,e,f}$  for Alice and Bob) on observing  $(e, f)$  by first fixing  $E = e$  and then taking the conditional distribution on  $F = f$ . It is not hard to show that  $P_{AB|XY,e,f}$  defined above is still a NS-strategy for Alice and Bob. Furthermore, one could extend the conditional strategy definition to handle any event  $= \{(e_i, f_i) : i = 1, \dots\}$  on Eve’s side by setting

$$P_{AB|XY,\text{event}} = \sum_i \Pr[e_i, f_i | \text{event}] P_{AB|XY,e_i,f_i}, \quad (\text{A.1})$$

which is also a NS-strategy for Alice and Bob.

**Martingale.** Define a *filter*  $\{\mathcal{F}_i : i = 0, \dots, n\}$  as an increasing sequence of  $\sigma$ -fields such that  $\emptyset = \mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \dots \subseteq \mathcal{F}_n$  on some probability space. Let  $\{X_i\}$  be a sequence of random variables such that  $X_i$  is measurable with respect to  $\mathcal{F}_i$ . We call  $\{X_i\}$  a *martingale* with respect to  $\{\mathcal{F}\}$  if  $\forall i, E[X_i | \mathcal{F}_{i-1}] = X_{i-1}$ .

**Lemma A.1 (Azuma-Hoeffding)** *Let  $X$  be a martingale associated with a filter  $\mathbf{F}$  such that  $|x_k - x_{k-1}| \leq c_k$  for all  $k$ . Then for all integers  $m$  and  $\lambda \geq 0$ ,*

$$\Pr[X_m \leq \mathbb{E}[X_m] - \lambda] \leq e^{-\frac{\lambda^2}{2(\sum_{k=1}^m c_k^2)}}. \quad (\text{A.2})$$

## A.1 Strong Monogamy of BHK games

### BHK Games

The  $\text{BHK}_M$  game (parameterized by  $M$ ), introduced in [BHK05], proceed as follows. Two spatially separated players, Alice and Bob, receive  $X, Y \in \{0, \dots, M-1\}$  and output  $A, B \in \{0, 1\}$  respectively. Any input pair  $(X, Y)$  is valid if and only if it is from the set  $\text{Input}_{\text{BHK}_M} = \{(x, y) : y = x \text{ or } y = x + 1 \text{ mod } M\}$ . Let the indicator function  $I$  be defined as  $I\{\text{true}\} = 1$ ,  $I\{\text{false}\} = 0$ . For any input-output pair  $(X, Y, A, B)$ , the game value  $\mathcal{B}$  is defined as

$$\mathcal{B}[A, B, X, Y] = \frac{1}{2} + M(A \oplus B \oplus I\{X = M-1\}I\{Y = 0\}). \quad (\text{A.3})$$

The expected game value, denoted  $\langle \mathcal{B} \rangle$ , is over *uniformly* selected valid inputs. One could define the game value vector  $|\text{BHK}_M\rangle$  such that

$$\langle \mathcal{B} \rangle = \langle \text{BHK}_M, P_{AB|XY} \rangle, \quad (\text{A.4})$$

where  $P_{AB|XY}$  is any NS-strategy for  $\text{BHK}_M$  games. Let us consider  $\langle \mathcal{B} \rangle$  obtained by *classical* and *quantum* strategies for this game.

**Classical Strategies.** Without loss of generality, one can restrict to *deterministic* strategies. It is easy to see that any deterministic strategy will incur a penalty of  $M$  on at least one valid input, which happens with probability  $1/2M$ . Thus the expected game value  $\langle \mathcal{B} \rangle$  satisfies,

$$\langle \mathcal{B} \rangle \geq \frac{1}{2} + M \frac{1}{2M} = 1.$$

**Quantum Strategies.** There turns out to be a good quantum strategy for  $\text{BHK}_M$  games achieving the following expected game value,

$$\langle \mathcal{B} \rangle = \frac{1}{2} + M \sin^2\left(\frac{\pi}{4M}\right) = \frac{1}{2} + O\left(\frac{1}{M}\right). \quad (\text{A.5})$$

The particular quantum strategy is as follows. Let Alice and Bob share an EPR pair. For any  $x \in \{0, \dots, M-1\}$  for Alice, she performs the measurement in the orthogonal basis,

$$\{|0\rangle \mp e^{i\pi \frac{x}{M}} |1\rangle\}_{x \in \{0, \dots, M-1\}},$$

while for any  $y \in \{0, \dots, M-1\}$  for Bob, he performs the measurement in the orthogonal basis,

$$\{|0\rangle \mp e^{-i\pi \frac{y+1/2}{M}} |1\rangle\}_{y \in \{0, \dots, M-1\}}.$$

Thus for each valid input  $(x, y)$ , the strategy loses with probability  $\sin^2(\frac{\pi}{4M})$ , which leads to Equ. (A.5).

**Representation of NS-Strategies.** Now we turn to a few properties of the representation of any non-signaling (NS) strategy for  $\text{BHK}_M$  games, which were discovered in [MRC<sup>+</sup>06]. Adopting the notation in [MRC<sup>+</sup>06], we arrange any NS-strategy  $P_{AB|XY}$  vector as follows,

$$P_{A,B|X,Y} = \begin{array}{|c|c|c|c|} \hline P(0,0|0,0) & P(0,1|0,0) & \dots & P(0,0|0,M-1) \\ \hline P(1,0|0,0) & P(1,1|0,0) & & \\ \hline \vdots & & \ddots & \vdots \\ \hline P(0,0|M-1,0) & \dots & & P(0,0|M-1,M-1) \\ \hline \end{array} \quad (\text{A.6})$$

Moreover, we define two vectors  $\vec{\mathbf{1}}, \nu$  of the same dimension as

$$\vec{\mathbf{1}} = \begin{array}{|c|c|c|c|} \hline \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} & \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} & & \\ \hline & \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} & \ddots & \\ \hline & & \ddots & \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \\ \hline \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} & & & \begin{array}{cc} 1 & 1 \\ 1 & 1 \end{array} \\ \hline \end{array}, \quad \nu = \frac{1}{2} \begin{array}{|c|c|c|c|} \hline \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} & \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} & & \\ \hline & \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} & \ddots & \\ \hline & & \ddots & \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \\ \hline \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} & & & \begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array} \\ \hline \end{array}, \quad (\text{A.7})$$

where empty boxes are understood as having zeros

$$\boxed{\phantom{00}} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad (\text{A.8})$$

and ellipsis between two identical boxes are understood as an arbitrarily large sequence of identical boxes. In the following, we demonstrate a connection between Alice's input-output distribution and the expected game value. Let  $\mu = \frac{1}{4M} \vec{\mathbf{1}}$ . For any  $a \in \{0, 1\}$ , define

$$\beta_a = \mu + (-1)^a \nu. \quad (\text{A.9})$$

Moreover, we have

$$|\text{BHK}_M\rangle = \mu + |\nu|, \quad (\text{A.10})$$

where  $|\nu|$  means entry-wise absolute value. It is easy to see that  $\beta_a \preceq |\text{BHK}_M\rangle, \forall a \in \{0, 1\}$ , where " $\preceq$ " means entry-wise " $\leq$ ".

Now imagine one play  $k$   $\text{BHK}_M$  games over  $k$  pairs of separate boxes in parallel (denote such a game by  $\text{BHK}_M^k$ ) and assign the game value according to the vector  $|\text{BHK}_M^k\rangle = |\text{BHK}_M\rangle^{\otimes k}$ . Similarly, for any  $\mathbf{a} \in \{0, 1\}^k$ , one could define

$$\beta_{\mathbf{a}} = \bigotimes_{i=1}^k \beta_{a_i}. \quad (\text{A.11})$$

The following lemma provides an alternative characterization of Alice's side input-output distribution  $\mathbf{P}_{\mathbf{a}|\mathbf{x}}$  in terms of  $\beta_{\mathbf{a}}$  and  $\mathbf{P}_{\mathbf{AB}|\mathbf{XY}}$ .

**Lemma A.2** ([MRC<sup>+</sup>06], Lemma 6) *Assume  $\mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$  is an arbitrary  $2k$ -partite non-signaling strategy, then for any  $\mathbf{a} \in \{0,1\}^k$  and any  $\mathbf{x} \in \{0, \dots, M-1\}^{\otimes k}$ , we have*<sup>9</sup>

$$\mathbf{P}_{\mathbf{a}|\mathbf{x}} = \beta_{\mathbf{a}} \cdot \mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}. \quad (\text{A.12})$$

Observe that, by definition, we have

$$\beta_{\mathbf{a}} = \beta_{a_1} \otimes \beta_{a_2} \otimes \dots \otimes \beta_{a_k} \preceq |\text{BHK}_M^k\rangle^{\otimes k} = |\text{BHK}_M^k\rangle. \quad (\text{A.13})$$

Also note that all entries in  $\mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$  are nonnegative, thus we have

**Corollary A.3** *For any  $\mathbf{a} \in \{0,1\}^k$  and any  $\mathbf{x} \in \{0, \dots, M-1\}^{\otimes k}$ , we have*

$$\mathbf{P}_{\mathbf{a}|\mathbf{x}} \leq \langle \text{BHK}_M^k, \mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} \rangle. \quad (\text{A.14})$$

Let  $\beta_{\text{uniform}} = (\frac{1}{2M}\vec{\mathbf{1}})^{\otimes k}$ , which is a normalized "uniform" vector over all valid inputs and satisfies

$$\beta_{\text{uniform}} \cdot \mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} = 1, \quad (\text{A.15})$$

for any NS-strategy  $\mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$  for  $\text{BHK}_M^k$  games. Moreover, we have

$$\sum_{\mathbf{a} \in \{0,1\}^k} \beta_{\mathbf{a}} = \left( \frac{1}{2M}\vec{\mathbf{1}} \right)^{\otimes k} = \beta_{\text{uniform}}. \quad (\text{A.16})$$

## Strong Monogamy

In this section we modularize and extend the technique in [Mas09] about a strong *monogamy* phenomenon of  $\text{BHK}_M^k$  games. Roughly, it says that if one plays  $\text{BHK}_M^k$  very well, then there exists a function  $h : \{0,1\}^k \rightarrow \{0,1\}$  such that the bit  $h(\mathbf{a})$ , obtained from Alice's output  $\mathbf{a}$ , is almost uniform against the environment, no matter how Alice, Bob, and the environment are correlated. We formulate this technique for  $\text{BHK}_M^k$  games and provide an *efficient* way to find such a function  $h$ . We remark this strong monogamy phenomenon plays a *crucial* role in our protocol in Fig. (4).

**Settings.** Assume  $\rho_{ABE} \in \text{Dens}(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{E})$  is a three-partite quantum state, in which  $\mathcal{A} \otimes \mathcal{B}$  denotes Alice and Bob who are playing  $\text{BHK}_M^k$  games, and  $\mathcal{E}$  denotes the environment. Let  $\mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}$  be any NS-strategy<sup>10</sup> for  $\text{BHK}_M^k$  games. We then apply *some* function  $h : \{0,1\}^k \rightarrow \{0,1\}$  to Alice's output  $\mathbf{a} \in \{0,1\}^k$  (given input  $\mathbf{x}$ ) and output  $z = h(\mathbf{a})$ , which leads to the state  $\rho_{ZE} \in \text{Dens}(\mathbb{C}^2 \otimes \mathcal{E})$ . We abstract the above process as an admissible super-operator  $\Phi_{\text{BHK}}^{\mathbf{x},h} : \text{L}(\mathcal{A} \otimes \mathcal{B}) \rightarrow \text{L}(\mathbb{C}^2)$  such that

$$\Phi_{\text{BHK}}^{\mathbf{x},h} \otimes \text{id}_{\mathcal{E}}(\rho_{ABE}) = \rho_{ZE}. \quad (\text{A.17})$$

Let  $\mathcal{A}_z = \{\mathbf{a} \in \{0,1\}^k : h(\mathbf{a}) = z\}$  for any  $z \in \{0,1\}$  and  $\beta_{\mathcal{A}_z} = \sum_{\mathbf{a} \in \mathcal{A}_z} \beta_{\mathbf{a}}$ . It follows from Lemma A.2 that the distribution of  $z$  (i.e.,  $\mathbf{P}_{z|\mathbf{x}}$ ) is given by

$$\mathbf{P}_{z|\mathbf{x}} = \sum_{\mathbf{a} \in \mathcal{A}_z} \mathbf{P}_{\mathbf{a}|\mathbf{x}} = \sum_{\mathbf{a} \in \mathcal{A}_z} \beta_{\mathbf{a}} \cdot \mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}} = \beta_{\mathcal{A}_z} \cdot \mathbf{P}_{\mathbf{A},\mathbf{B}|\mathbf{X},\mathbf{Y}}. \quad (\text{A.18})$$

The particular function  $h$  in our consideration should satisfy the following property.

<sup>9</sup>The original statement of Lemma 6 in [MRC<sup>+</sup>06] claims only for input  $\mathbf{x} = (0, \dots, 0)$ . However, one can invoke the relabeling technique demonstrated in Lemma 7 of the same paper to extend the statement to all  $\mathbf{x}$ s.

<sup>10</sup>This NS-strategy should be implementable by choosing appropriate POVMs and applying to the specific state  $\rho_{AB}$ .

**Property A.4 (Concentration)** Any function  $h : \{0, 1\}^k \rightarrow \{0, 1\}$  is  $C$ -concentrated if and only if for any  $z \in \{0, 1\}$  such that,

$$\left| \beta_{A_z} - \frac{1}{2} \beta_{\text{uniform}} \right| \preceq C \left| \text{BHK}_M^k \right\rangle. \quad (\text{A.19})$$

**Proposition A.5** Let  $\mathbf{P}_{\text{AB}|\text{XY}}$  be Alice and Bob's strategy for  $\text{BHK}_M^k$  games and  $h : \{0, 1\}^k \rightarrow \{0, 1\}$  is  $C$ -concentrated. Let  $\mathbf{a} \in \{0, 1\}^k$  be Alice's output given any input  $\mathbf{x}$ . The resultant state  $\rho_{ZE}$  (as defined in Equ.(A.17)) after outputting  $Z = h(\mathbf{a})$  satisfies,

$$\|\rho_{ZE} - \mathcal{U}_1 \otimes \rho_E\|_{\text{tr}} \leq 2C \left\langle \text{BHK}_M^k, \mathbf{P}_{\text{AB}|\text{XY}} \right\rangle. \quad (\text{A.20})$$

**Proof.** Our proof is almost identical to [Mas09] except that we express our statement in terms of quantum states. Due to the following fact,

**Fact A.6** Let  $\rho_0, \rho_1$  be two quantum states which appear with equal chance, the optimal success probability of predicting which state it is by a POVM is  $\frac{1}{2} + \frac{1}{4} \|\rho_0 - \rho_1\|_{\text{tr}}$ .

we have that  $\frac{1}{4} \|\rho_{ZE} - \mathcal{U}_1 \otimes \rho_E\|_{\text{tr}}$  to the best quantum advantage to distinguish between  $\rho_{ZE}$  and  $\mathcal{U}_1 \otimes \rho_E$  each appearing with probability  $1/2$ . Note that  $\rho_{ZE}$  (or  $\mathcal{U}_1 \otimes \rho_E$ ) is a cq-state and the most general approach to distinguish between these two states is to first read  $z$  and then apply the corresponding POVM on  $\mathcal{E}$  respectively. Let us pick the *best* quantum strategy in which when we apply POVM I on  $\mathcal{E}$  when  $z = 0$ , and apply POVM II when  $z = 1$ . Let  $f$  denote the outcome of these POVMs. Let  $p(z, f)$  (resp.  $q(z, f)$ ) be the distribution of  $(z, f)$  when applying the above strategy to  $\rho_{ZE}$  (resp.  $\mathcal{U}_1 \otimes \rho_E$ ). It is well known that

$$\|\rho_{ZE} - \mathcal{U}_1 \otimes \rho_E\|_{\text{tr}} = \sum_{z, f} |p(z, f) - q(z, f)|.$$

Let us imagine the NS-strategy (denoted  $\mathbf{P}_{\text{ABF}|\text{XYE}}$ ) among Alice, Bob, and the environment obtained as follows. Initially, they share the state  $\rho_{ABE}$ . Then Alice and Bob choose POVMs to play  $\text{BHK}_M^k$  games and the environment performs POVM I/II when its input  $E = 0/1$ . It is easy to see that  $q(z, f)$  is only related to  $\mathbf{P}_{F|E}$  in the following way,

$$q(z, f) = \frac{1}{2} \mathbf{P}_{f|e(z)}.$$

It is a little trickier to connect  $p(z, f)$  to  $\mathbf{P}_{\text{ABF}|\text{XYE}}$ . Let  $\mathbf{P}_{\text{ZF}|\text{XE}}$  denote the effective NS-strategy by outputting  $Z = h(\mathbf{a})$  obtained from  $\mathbf{P}_{\text{ABF}|\text{XYE}}$ . For any fixed input  $\mathbf{x}, z, e, f$ , we have

$$\begin{aligned} \mathbf{P}_{z, f | \mathbf{x}, e} &= \mathbf{P}_{z | \mathbf{x}, e, f} \mathbf{P}_{f | \mathbf{x}, e} \\ &= (\beta_{A_z} \cdot \mathbf{P}_{\text{AB}|\text{XY}, e, f}) \mathbf{P}_{f | e}, \end{aligned}$$

where the second equality is due to Equ.(A.18) and the NS-condition  $\mathbf{P}_{f | \mathbf{x}e} = \mathbf{P}_{f | e}$ . By definition,  $p(z, f)$  is the probability when Alice and Bob obtain  $z$  (given  $\mathbf{x}$ ) and the environment performs the POVM according to  $z$  (i.e., choose  $E = e(z)$ ) and obtains  $f$ , namely

$$p(z, f) = \mathbf{P}_{z, f | \mathbf{x}, e(z)} = (\beta_{A_z} \cdot \mathbf{P}_{\text{AB}|\text{XY}, e(z), f}) \mathbf{P}_{f | e(z)}.$$

Thus, we have

$$\begin{aligned}
\sum_{z,f} |p(z,f) - q(z,f)| &= \sum_{z,f} \mathbf{P}_{f|e(z)} \left| \beta_{\mathcal{A}_z} \cdot \mathbf{P}_{\mathbf{AB}|\mathbf{XY},e(z),f} - \frac{1}{2} \right| \\
&\leq \sum_{z,f} \mathbf{P}_{f|e(z)} \left| \beta_{\mathcal{A}_z} - \frac{1}{2} \beta_{\text{uniform}} \right| |\mathbf{P}_{\mathbf{AB}|\mathbf{XY},e(z),f}\rangle \\
&\leq C \left\langle \text{BHK}_M^k, \sum_{z,f} \mathbf{P}_{f|e(z)} \mathbf{P}_{\mathbf{AB}|\mathbf{XY},e(z),f} \right\rangle \\
&= 2C \left\langle \text{BHK}_M^k, \mathbf{P}_{\mathbf{AB}|\mathbf{XY}} \right\rangle,
\end{aligned}$$

where the second inequality is from Equ.(A.15) and the convexity of the absolute value function. The third inequality is because  $h$  is  $C$ -concentrated. The last equality is because  $\sum_f \mathbf{P}_{f|e} \mathbf{P}_{\mathbf{AB}|\mathbf{XY},e,f} = \sum_f \mathbf{P}_{\mathbf{AB}f|\mathbf{XY}e} = \mathbf{P}_{\mathbf{AB}|\mathbf{XY}}$  for any  $e$  by NS-conditions.  $\blacksquare$

Then it suffices to find  $C$ -concentrated functions with reasonable  $C$ s. It was found in [Mas09] that fully random hashing functions from  $\{0,1\}^k$  to  $\{0,1\}$  are  $2^{O(\sqrt{k})}$ -concentrated. However, generating such hashing functions requires  $2^k$  uniform bits. In the following we claim that  $\Theta(k)$ -wise random hashing functions (requiring only  $\Theta(k)$  uniform bits to generate) are reasonably concentrated, which leads to an *efficient* protocol to generate desired functions. To that end, we build a concentration bound about the summation of any  $t$ -wise independent random variables in Lemma A.7 and prove our main claim in Lemma A.8.

**Lemma A.7** *Let  $t \geq 4$  be even. Let  $X_1, \dots, X_n$  be  $t$ -wise independent random variables over  $[-1, 1]$  with  $\mathbb{E}[X_i] = 0$  and  $\text{Var}[X_i] \leq \sigma$  for every  $i \in [n]$ . Let  $X = \sum_i X_i$ . If  $\sigma n \geq 2$  then for every  $C > 0$ , we have*

$$\Pr[|X| \geq C] \leq \left( \frac{\sigma n t^2}{4C^2} \right)^{t/2}.$$

**Proof.** By a standard moment method, we have

$$\Pr[|X| \geq C] = \Pr[X^t \geq C^t] \leq \frac{\mathbb{E}[X^t]}{C^t}.$$

By definition and linearity of expectation,

$$\mathbb{E}[X^t] = \mathbb{E} \left[ \left( \sum_{i=1}^n X_i \right)^t \right] = \sum_{i_1, \dots, i_t} \mathbb{E}[X_{i_1} \cdots X_{i_t}]. \quad (\text{A.21})$$

For each term, if  $(i_1, \dots, i_t)$  consists of  $d$  distinct indices, then we can write

$$\mathbb{E}[X_{i_1} \cdots X_{i_t}] = \mathbb{E}[X_{j_1}^{a_1} \cdots X_{j_d}^{a_d}] = \mathbb{E}[X_{j_1}^{a_1}] \cdots \mathbb{E}[X_{j_d}^{a_d}]$$

for some indices  $j_1, \dots, j_d \in [n]$  and exponents  $a_1, \dots, a_d \geq 1$ , where the last equality uses  $t$ -wise independence. Note that  $X_i \in [-1, 1]$ ,  $\mathbb{E}[X_i] = 0$  and  $\text{Var}[X_i] \leq \sigma$  implies that  $|\mathbb{E}[X_i^a]| \leq \sigma$  for every  $a \geq 2$ . Thus, we have  $\mathbb{E}[X_{j_1}^{a_1}] \cdots \mathbb{E}[X_{j_d}^{a_d}] \leq \sigma^d$ . Also note that if  $(i_1, \dots, i_t)$  consists of more than  $t/2$  distinct indices, then there must exist some index  $i^*$  that appears only once, and since  $\mathbb{E}[X_{i^*}] = 0$ , the



term equals to 0. Finally, note that there are at most  $\binom{n}{d} \cdot d^t$  terms that consists of *exactly*  $d$  distinct indices. We can upper bound the sum in Eq. (A.21) by

$$\sum_{d=1}^{t/2} \sigma^d \cdot \binom{n}{d} \cdot d^t \leq \sum_{d=1}^{t/2} \frac{\sigma^d n^d}{2^d} \left(\frac{t}{2}\right)^t \leq \left(\frac{\sigma n t^2}{4}\right)^{t/2}.$$

Therefore,

$$\Pr[|X| \geq C] \leq \frac{\mathbb{E}[X^t]}{C^t} \leq \left(\frac{\sigma n t^2}{4C^2}\right)^{t/2}.$$

■

**Lemma A.8** Any  $t$ -wise random hash function  $h : \{0, 1\}^k \rightarrow \{0, 1\}$  is  $2^{\frac{1}{2}(k+O(\log(k)))}$ -concentrated with probability  $1 - 2^{-\Omega(k)}$  when  $t = \Theta(k)$ .

**Proof.** We shall first prove the *concentration* property holds for any fixed  $z \in \{0, 1\}$  and any entry of  $\beta_{\mathcal{A}_z}$  and then invoke union bounds to show the very property holds for all  $z$  and all entries.

Let a tuple  $\tau = (\mathbf{a}, \mathbf{b}, \mathbf{x}, \mathbf{y})$  be an index of entries of  $\beta_{\mathcal{A}_z}$ . Denote the corresponding entry by  $\beta_{\mathcal{A}_z}^\tau$ . It suffices to only consider indices corresponding to valid inputs  $(\mathbf{x}, \mathbf{y})$ . For invalid inputs  $(\mathbf{x}, \mathbf{y})$ , we have  $\beta_{\mathcal{A}_z}^\tau = \beta_{\text{uniform}}^\tau = 0$  and thus the property holds trivially.

Let us characterize any  $t$ -wise random hash function  $h$  by a collection of  $t$ -wise independent random variables  $\{V_{\mathbf{a}}\}_{\mathbf{a} \in \{0, 1\}^k}$ . For any fixed  $z \in \{0, 1\}$ , let  $V_{\mathbf{a}}$  be the indicator whether  $h(\mathbf{a}) = z$ . Moreover,  $V_{\mathbf{a}} = 0$  or  $1$  with probability  $1/2$ . Thus the entry  $\beta_{\mathcal{A}_z}^\tau$  can be represented by

$$\beta_{\mathcal{A}_z}^\tau = \sum_{\mathbf{a} \in \mathcal{A}_k} \beta_{\mathbf{a}}^\tau = \sum_{\mathbf{a} \in \{0, 1\}^k} V_{\mathbf{a}} \beta_{\mathbf{a}}^\tau. \quad (\text{A.22})$$

By linearity of expectation, we have

$$\mathbb{E}[\beta_{\mathcal{A}_z}^\tau] = \sum_{\mathbf{a} \in \{0, 1\}^k} \mathbb{E}[V_{\mathbf{a}}] \beta_{\mathbf{a}}^\tau = \frac{1}{2} \sum_{\mathbf{a} \in \{0, 1\}^k} \beta_{\mathbf{a}}^\tau = \frac{1}{2} \beta_{\text{uniform}}^\tau, \quad (\text{A.23})$$

where we makes use of  $\mathbb{E}[V_{\mathbf{a}}] = 1/2$  and Equ. (A.16). In the following we prove that  $\beta_{\mathcal{A}_z}^\tau$  is concentrated around its expectation with the help of Lemma A.7. Let  $Y_{\mathbf{a}} = V_{\mathbf{a}} \beta_{\mathbf{a}}^\tau$  and  $X_{\mathbf{a}} = (Y_{\mathbf{a}} - \mathbb{E}[Y_{\mathbf{a}}]) / |\text{BHK}_M^k\rangle^\tau$ . Note that  $|\beta_{\mathbf{a}}| \preceq |\text{BHK}_M^k\rangle$  and thus  $|Y_{\mathbf{a}}| \leq \beta_{\mathbf{a}}^\tau \leq |\text{BHK}_M^k\rangle^\tau$ . Thus we have that  $\mathbb{E}[X_{\mathbf{a}}] = 0$  and  $X_{\mathbf{a}} \in [-1, 1]$ . Moreover,

$$\text{Var}[X_{\mathbf{a}}] = \frac{1}{(|\text{BHK}_M^k\rangle^\tau)^2} \text{Var}[Y_{\mathbf{a}}] \leq \frac{1}{(|\text{BHK}_M^k\rangle^\tau)^2} \mathbb{E}[Y_{\mathbf{a}}^2] = \frac{(\beta_{\mathbf{a}}^\tau)^2}{(|\text{BHK}_M^k\rangle^\tau)^2} \mathbb{E}[V_{\mathbf{a}}^2] \leq \frac{1}{2}. \quad (\text{A.24})$$

Now we apply Lemma A.7 to the collection  $\{X_{\mathbf{a}} : \mathbf{a} \in \{0, 1\}^k\}$  with  $\sigma = 1/2$ ,  $n = 2^k$ ,  $C = 2^{\frac{1}{2}(k+O(\log(k)))}$ , and  $t = \Theta(k)$ . Then we have

$$\Pr \left[ \left| \sum_{\mathbf{a} \in \{0, 1\}^N} X_{\mathbf{a}} \right| \geq C \right] \leq \left( \frac{2^{k-1} t^2}{4C^2} \right)^{t/2} \leq 2^{-\Omega(k)}. \quad (\text{A.25})$$

---

**Protocol  $\Pi_{\text{BHK}}$**

1. Let  $S$  be the random bits and parameters  $\epsilon_B, \gamma, M$ , both be given as input. Let  $k = \Theta(\log(1/\epsilon_B))$ ,  $\alpha = \left(\frac{1-\gamma}{\sqrt{2}}\right)^k$ ,  $c = (\frac{1}{2} + M)^k$  and  $n = \Theta(c^2 \log(1/\epsilon_B)/\alpha^2)$ . The input randomness  $S$  of length  $\Theta(nk)$  is split into  $(\mathbf{X}, \mathbf{Y}, R, H)$ .
  2. Run  $\text{BHK}_M^k$  games for  $n$  times in parallel on  $n \times k$  pairs of spatially separated boxes (nonlocal boxes) with random valid inputs generated from  $\mathbf{X}, \mathbf{Y}$ .
  3. Let  $w_1, \dots, w_n \in [k]$  denote the number of acceptances in each  $\text{BHK}_M^k$  game and define  $v_i = (1/2)^{w_i} \cdot (1/2 + M)^{k-w_i}$  for  $i \in [n]$ .
  4. Use  $R$  to select a uniformly random index  $r \in [n]$ . Let  $v_{-r} = \sum_{i \neq r} v_i$ .
    - 4.1 If  $v_{-r} \leq \alpha n$ , then **Accept**. Moreover, use  $H$  to generate a  $\Theta(k)$ -wise independent hash function  $h : \{0, 1\}^k \rightarrow \{0, 1\}$ , then output  $h(\mathbf{a}_r)$  where  $\mathbf{a}_r$  is Alice side's output of the  $r$ th  $\text{BHK}_M^k$  game.
    - 4.2 Otherwise, **Reject**.
- 

Figure 4: Protocol  $\Pi_{\text{BHK}}$  from  $\text{BHK}_M^k$  games.

Note that the event  $|\sum_{\mathbf{a} \in \{0,1\}^k} X_{\mathbf{a}}| \geq C$  is equivalent to the event  $|\beta_{\mathcal{A}_z}^\tau - \mathbb{E}[\beta_{\mathcal{A}_z}^\tau]| \geq C |\text{BHK}_M^k\rangle^\tau$ . Thus for any  $z \in \{0, 1\}$  and any index  $\tau$ , we have

$$\Pr \left[ \left| \beta_{\mathcal{A}_z}^\tau - \frac{1}{2} \beta_{\text{uniform}}^\tau \right| \leq C |\text{BHK}_M^k\rangle^\tau \right] \geq 1 - 2^{-\Omega(k)}. \quad (\text{A.26})$$

By union bounds over all  $z$  and indices  $\tau$  and note that  $M$  is constant, we have

$$\Pr_h \left[ \bigwedge_{z \in \{0,1\}} \left\{ \left| \beta_{\mathcal{A}_z} - \frac{1}{2} \beta_{\text{uniform}} \right| \leq 2^{\frac{1}{2}(k+O(\log(k)))} |\text{BHK}_M^k\rangle \right\} \right] \geq 1 - 2^{-\Omega(k)+\log(8M)k} = 1 - 2^{-\Omega(k)}, \quad (\text{A.27})$$

which completes the proof. ■

## B A Concrete Strong Randomness Certification Protocol

In this section, we construct a concrete randomness certification protocol based on BHK games, the relevant knowledge of which is surveyed in Appendix A.1. We *directly* prove its strong soundness, instead of invoking Lemma 4.6, by making use of a *strong monogamy* phenomenon of BHK games. The protocol (denoted  $\Pi_{\text{BHK}}$ ) proceeds as in Figure 4. The parameter  $\epsilon_B$  is the soundness parameter of this protocol, while  $\gamma$  is some parameter related to the robustness and  $M$  is the parameter for BHK games.

The following of this section is organized as follows. We discuss the completeness and robustness of this protocol in Appendix B.1. We devote Appendix B.2 to the analysis of the strong soundness of this protocol and prove the main soundness theorem in Theorem B.4.

## B.1 Completeness and Robustness

Our design of protocol  $\Pi_{\text{BHK}}$  requires  $v_{-r} \leq \alpha n$  to accept. For honest boxes, this roughly requires each play of the  $\text{BHK}_M$  game (not  $\text{BHK}_M^k$ ) must obtain game value no more than  $\frac{1-\gamma}{\sqrt{2}}$ . Let  $0 \leq \delta_n \leq 1$  denote the noise parameter in the same sense as Theorem 4.4. Namely, each round's output of playing  $\text{BHK}_M$  game might be changed with  $\delta_n$  chance.

**Completeness.** The completeness of  $\Pi_{\text{BHK}}$  can be achieved by invoking the quantum strategy demonstrated in Appendix A.1, which achieves the rejection probability  $\sin^2(\frac{\pi}{4M})$  for each play of  $\text{BHK}_M$  game, for whatever input  $(x, y)$ . Taking into account the noise  $\delta_n$ , thus for each play of  $\text{BHK}_M$  game, the honest boxes can achieve game values no more than

$$\frac{1}{2} + M \left( \sin^2 \left( \frac{\pi}{4M} \right) + \delta_n \right),$$

which is smaller than  $\frac{1-\gamma}{\sqrt{2}}$  by choosing appropriate  $M$  and small enough  $\gamma$  and  $\delta_n$ . When this condition is achieved, by concentration of measures, we have for this strategy, the protocol  $\Pi_{\text{BHK}}$  accepts with probability  $1 - 2^{-\Omega(nk)}$  on whatever source.

**Robustness.** To optimize robustness, it suffices to choose appropriate  $M, \gamma, \delta_n$  that satisfy the following constraint and maximize  $\delta_n$ ,

$$\frac{1}{2} + M \left( \sin^2 \left( \frac{\pi}{4M} \right) + \delta_n \right) \leq \frac{1-\gamma}{\sqrt{2}}.$$

It follows easily that one can choose  $M = 6$ ,  $\gamma = 10^{-8}$  to get  $\delta_n \approx 1.748\%$ .

## B.2 Soundness analysis of $\Pi_{\text{BHK}}$

Let us analyze  $\Pi_{\text{BHK}}$  with some initial state  $\xi \in \text{Dens}(S \otimes \mathcal{D} \otimes \mathcal{E})$ , where  $S$  denotes the randomness space,  $\mathcal{D}$  is the system of Alice and Bob's boxes, and  $\mathcal{E}$  is the rest of the world (which could include the system of other runs of Protocol B and the adversary). Moreover, we assume that

$$\xi_{SD} = \mathcal{U}_S \otimes \xi_D, \tag{B.1}$$

where  $\xi_{SD}$  is the reduced state on  $S \otimes \mathcal{D}$  system. However,  $\xi_{SD}$  might be correlated with  $\mathcal{E}$  system. Note that  $S$  is classical, thus the most general correlation between  $S \otimes \mathcal{D}$  and  $\mathcal{E}$  can be expressed as,

$$\xi_{SDE} = \sum_s p_s |s\rangle\langle s| \otimes \xi_{DE}^s. \tag{B.2}$$

Due to Equ.(B.1), we have that  $\text{tr}_{\mathcal{E}}(\xi_{DE}^s) = \xi_D$  and  $p_s = \frac{1}{\dim(S)}$ . During the running of Protocol B, the underlying quantum state (especially its correlation with  $\mathcal{E}$  system) at any intermediate step should be in the following form

$$\sum_{\tau} p_{\tau} |\tau\rangle\langle \tau| \otimes \xi_{\tilde{D}E}^{\tau}, \tag{B.3}$$

where  $\tau$  is classical and  $\tilde{D}$  is part of  $\mathcal{D}$  system that has not yet been operated on. Moreover, since  $\Phi_B$  only applies on  $S \otimes \mathcal{D}$  system, thus  $p_{\tau}$  only depends on  $\Phi_B$  and  $\xi_{SD}$ . This observation allows us to calculate the value of some  $p_{\tau}$  by looking at  $\xi_{SD}$  system only.

Let  $\mathbf{P}_{\mathbf{AB}|\mathbf{XY}}$  be the NS-strategy of boxes to play  $n$   $\text{BHK}_M^k$  games. Moreover, for analysis purpose, we give  $n$   $\text{BHK}_M^k$  games an *artificial* order and imagine  $\text{BHK}_M^k$  games are played sequentially (though on different boxes) in this order.

**Probability Space.** We are interested in the case  $\tau = (\mathbf{X}, \mathbf{Y}, R, H, \mathbf{A}, \mathbf{B})$  from Equ.(B.3). Note that  $S$  already contains  $\mathbf{X}, \mathbf{Y}, R, H$  and  $\mathbf{A}, \mathbf{B}$  are the outputs of  $n$   $\text{BHK}_M^k$  games given inputs  $\mathbf{X}, \mathbf{Y}$ . Moreover, at this moment, we have  $\tilde{D} = \emptyset$  and the whole system is similar to Equ.(B.3). Let us focus on the distribution of  $\tau$  which is given by  $\xi_{SD}$ . By Equ.(B.1),  $\mathbf{X}, \mathbf{Y}, R, H$  are independently sampled, and thus we have

$$\Pr[\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, R, H] = \Pr[R]\Pr[H]\Pr[\mathbf{X}]\Pr[\mathbf{Y}]\mathbf{P}_{\mathbf{A}, \mathbf{B}|\mathbf{X}, \mathbf{Y}}.$$

Let  $\text{cond}$  be a set of input-output pairs from some subset of the  $n$   $\text{BHK}_M^k$  games. We define the following set of random variables over the probability space  $(\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, R, H)$ . Initialize  $\text{cond}_0 = \emptyset$ . For each  $i = 1, \dots, n$ ,

- Let  $\mu_i = \mu_i(\text{cond}_{i-1}) = \langle \text{BHK}_M^k | \mathbf{P}_{\mathbf{A}_i, \mathbf{B}_i | \mathbf{X}_i, \mathbf{Y}_i, \text{cond}_{i-1}} \rangle$ <sup>11</sup>.
- Sample independently uniform bits  $\mathbf{x}_i, \mathbf{y}_i$  and sample  $\mathbf{a}_i, \mathbf{b}_i$  according to  $P_{\mathbf{A}_i, \mathbf{B}_i | \mathbf{x}_i, \mathbf{y}_i, \text{cond}_{i-1}}$ . Set  $\text{cond}_i = \text{cond}_{i-1} \circ (\mathbf{x}_i, \mathbf{y}_i, \mathbf{a}_i, \mathbf{b}_i)$ .
- Let  $w_i$  be the number of accepts in  $(\mathbf{x}_i, \mathbf{y}_i, \mathbf{a}_i, \mathbf{b}_i)$  and  $w_i = (1/2)^{w_i} \cdot (1/2 + M)^{k-w_i}$  (as in Fig. 4).

Let  $\mu = \sum_i \mu_i$  and  $v = \sum_i v_i$ . Sample  $r$  from  $R$  and let  $\mu_{-r} = \sum_{i \neq r} \mu_i$  and  $v_{-r} = \sum_{i \neq r} v_i$ . Let  $\text{Acc}$  denote the event that the protocol accepts (i.e., the event  $\{v_{-r} \leq \alpha n\}$ ). Let  $\text{Rej}$  denote the event otherwise. Let  $c = (1/2 + M)^k$ .

**Lemma B.1** *For every  $\delta \in (0, 1)$ , we have  $\Pr[v \leq \mu - \delta n] \leq e^{-\delta^2 n / 2c^2}$ .*

**Proof.** The lemma follows by observing that the random variables defined above forms a martingale and applying Lemma A.1. Formally, for  $i \in \{0, \dots, n\}$ , let  $\mathcal{F}_i$  be the  $\sigma$ -field generated by  $\text{cond}_i$ , which yields a natural filter  $\mathbf{F}$ :  $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \dots \subset \mathcal{F}_n$ . By definition, for every  $i \in [n]$  and  $\text{cond}_{i-1}$ ,  $\mathbb{E}[v_i | \text{cond}_{i-1}] = \mu_i(\text{cond}_{i-1})$ . Thus, define  $P_i \stackrel{\text{def}}{=} v_i - \mu_i$ , and  $Q_i = \sum_{j \leq i} P_j$  for  $i \in [n]$ , and we have that  $Q_0 = 0, Q_1, \dots, Q_n$  forms a martingale corresponding to the filter  $\mathbf{F}$  with  $|Q_i - Q_{i-1}| \leq c$ . By Lemma A.1 with  $\lambda = \delta n$  and note that  $\mathbb{E}[Q_n] = 0$ , we have

$$\Pr[Q_n \leq -\delta n] \leq e^{-\frac{\lambda^2}{2nc^2}} \leq e^{-\delta^2 n / 2c^2}.$$

By definition,  $Q_n = v - \mu$ , thus we have  $\Pr[v \leq \mu - \delta n] \leq e^{-\delta^2 n / 2c^2}$ . ■

**Lemma B.2** *For every  $\alpha, \delta, \epsilon_1, \epsilon_2, \epsilon_3 \in (0, 1)$  such that  $\epsilon_1 \cdot \epsilon_2 \geq e^{-\delta^2 n / 2c^2}$  and let  $\eta = \alpha + \delta + c/n$ , if  $\Pr[\text{Acc}] \geq \epsilon_1$ , then*

$$\Pr[\mu_r \leq \eta / \epsilon_3 | \text{Acc}] \geq 1 - \epsilon_2 - \epsilon_3.$$

---

<sup>11</sup> $\mathbf{P}_{\mathbf{A}_i, \mathbf{B}_i | \mathbf{X}_i, \mathbf{Y}_i, \text{cond}_{i-1}}$  should be understood as the conditional NS-strategy for the  $i$ th game on the event  $\text{cond}_{i-1}$ .

**Proof.** Recall that the protocol accepts when  $v_{-r} \leq \alpha n$ , which implies  $v \leq \alpha n + c$ . Lemma B.1 implies that

$$\Pr[\text{Acc} \wedge \mu \geq (\alpha + \delta)n + c = \eta n] \leq e^{-\delta^2 n / 2c^2}.$$

Thus, if  $\Pr[\text{Acc}] \geq \epsilon_1$ , then

$$\Pr[\mu \leq \eta n | \text{Acc}] \geq 1 - e^{-\delta^2 n / 2c^2} / \epsilon_1 \geq 1 - \epsilon_2.$$

By Markov inequality, if  $\mu \leq \eta n$ , then there are at most  $\epsilon_3$ -fraction of  $\mu_i \geq \eta / \epsilon_3$ . Since  $r$  is a random index, thus we have

$$\Pr[\mu_r \leq \eta / \epsilon_3 | \text{Acc}] \geq 1 - \epsilon_2 - \epsilon_3. \quad \blacksquare$$

Let  $\mathcal{A}_i \otimes \mathcal{B}_i$  denote Alice and Bob's system for the  $i$ th  $\text{BHK}_M^k$  game. Namely  $\mathcal{D} = \bigotimes_{i=1}^n \mathcal{A}_i \otimes \mathcal{B}_i$ . By Protocol B, we shall sample a random  $r$  and choose the  $r$ th  $\text{BHK}_M^k$  game for output. Previously, we establish a bound about  $\mu_r(\text{cond}_{r-1})$ , namely, the NS-strategy for the  $r$ th game conditioned on the inputs and outputs (i.e.,  $\text{cond}_{r-1}$ ) of the first  $r-1$   $\text{BHK}_M^k$  games. However, this is insufficient for our purpose because we care about the NS-strategy in the  $\text{Acc}$  case. Note that all  $\text{BHK}_M^k$  games are played on *separated* boxes and the event  $\text{Acc}$  depends on all  $n$  games except the  $r$ th one. Thus it is valid to talk about the NS-strategy for the  $r$ th game conditioned  $\text{cond}_{r-1}$  and  $\text{Acc}$ . Let

$$\mu_r(\text{cond}_{r-1}, \text{Acc}) = \langle \text{BHK}_M^k | \mathbf{P}_{\mathbf{A}_r, \mathbf{B}_r | \mathbf{X}_r, \mathbf{Y}_r, \text{cond}_{r-1}, \text{Acc}} \rangle \quad (\text{B.4})$$

**Lemma B.3** *Let  $r$  be the random index in Protocol B, if  $\Pr[\text{Acc} | r, \text{cond}_{r-1}] > 0$ , then we have*

$$\mu_r(\text{cond}_{r-1}, \text{Acc}) \leq \frac{1}{\Pr[\text{Acc} | r, \text{cond}_{r-1}]} \mu_r(\text{cond}_{r-1}).$$

**Proof.** For every  $\mathbf{a}_r, \mathbf{b}_r, \mathbf{x}_r, \mathbf{y}_r$ , we have

$$\mathbf{P}_{\mathbf{a}_r, \mathbf{b}_r | \mathbf{x}_r, \mathbf{y}_r, \text{cond}_{r-1}, \text{Acc}} \leq \frac{\mathbf{P}_{\mathbf{a}_r, \mathbf{b}_r | \mathbf{x}_r, \mathbf{y}_r, \text{cond}_{r-1}}}{\Pr[\text{Acc} | \mathbf{x}_r, \mathbf{y}_r, r, \text{cond}_{r-1}]},$$

because  $\Pr[A | BC] \leq \Pr[A | B] / \Pr[C | B]$  for any event  $A, B, C$ . Note that  $\text{Acc}$  does not depend on the  $r$ th game. Moreover, by NS-condition and the fact  $\mathbf{x}_r, \mathbf{y}_r$  are independently sampled, different  $\mathbf{x}_r, \mathbf{y}_r$  won't disturb the input-output distribution of the rest  $n-1$  games. Thus, we have

$$\Pr[\text{Acc} | \mathbf{x}_r, \mathbf{y}_r, r, \text{cond}_{r-1}] = \Pr[\text{Acc} | r, \text{cond}_{r-1}]. \quad (\text{B.5})$$

By definition and note that all entries of  $|\text{BHK}_M^k\rangle$  are nonnegative, we have

$$\mu_r(\text{cond}_{r-1}, \text{Acc}) \leq \frac{1}{\Pr[\text{Acc} | r, \text{cond}_{r-1}]} \mu_r(\text{cond}_{r-1}). \quad \blacksquare$$

To prove our main claim in this section, let us consider the intermediate state  $\tilde{\xi} \in \text{Dens}(\tau \otimes \mathcal{D} \otimes \mathcal{E})$  (in the form of Equ.(B.3)) at the moment when all operations have been applied except for the  $r$ th game. Namely, if one applies  $\Phi_{\text{BHK}}^{\mathbf{x}_r, h}$  ( $h$  sampled from  $H$ ) to the corresponding part of  $\tilde{\xi}$  and outputs  $(\text{Acc}/\text{Rej}, Z)$ , then one obtains  $\Phi_A \otimes \text{id}_{\mathcal{E}}(\xi_{SDE})$ . Moreover, note that at this moment the protocol has already made its decision to accept or to reject. We thus only keep  $\tau = (\tau_1, \tau_2, \text{Acc}/\text{Rej})$  such that

$\tau_1 = (r, \text{cond}_{r-1})$  and  $\tau_2 = (\mathbf{x}_r, \mathbf{y}_r, h)$  and absorb other classical messages (such as  $\mathbf{x}_{>r}, \mathbf{y}_{>r}, \mathbf{a}_{>r}, \mathbf{b}_{>r}$ ) to the new environment  $E'$  (i.e.,  $E' = (\mathbf{x}_{>r}, \mathbf{y}_{>r}, \mathbf{a}_{>r}, \mathbf{b}_{>r}, E)$ ). Then, we have

$$\tilde{\xi} = \sum_{\tau_1, \tau_2} \mathbf{Pr}[\tau_1, \tau_2] |\tau_1, \tau_2\rangle \otimes \left( \mathbf{Pr}[\text{Acc}|\tau_1, \tau_2] |\text{Acc}\rangle \otimes \xi_{A_r B_r E'}^{\tau_1, \tau_2, \text{Acc}} + \mathbf{Pr}[\text{Rej}|\tau_1, \tau_2] |\text{Rej}\rangle \otimes \xi_{A_r B_r E'}^{\tau_1, \tau_2, \text{Rej}} \right), \quad (\text{B.6})$$

whose sub-normalized part  $\tilde{\xi}^{\text{Acc}}$  with  $|\text{Acc}\rangle$  is (re-order)

$$|\text{Acc}\rangle \otimes \tilde{\xi}^{\text{Acc}} = \mathbf{Pr}[\text{Acc}] |\text{Acc}\rangle \otimes \sum_{\tau_1, \tau_2} \mathbf{Pr}[\tau_1, \tau_2 | \text{Acc}] |\tau_1, \tau_2\rangle \otimes \xi_{A_r, B_r E'}^{\tau_1, \tau_2, \text{Acc}}. \quad (\text{B.7})$$

Note that the reduced state of  $\xi_{A_r B_r E'}^{\tau_1, \tau_2, \text{Acc}}$  on  $\tau \otimes \mathcal{D}$  system is  $\xi_{A_r, B_r}^{\tau_1, \text{Acc}}$ , which especially does not depend on  $\tau_2$  because of our assumption in Equ.(B.1) and the fact  $\tau_2$  has not yet been operated on until this moment. Thus, in the last step, the specific NS-strategy played on  $\xi_{A_r, B_r}^{\tau_1, \text{Acc}}$  is given by  $\mathbf{P}_{\mathbf{A}_r \mathbf{B}_r | \mathbf{X}_r \mathbf{Y}_r, \tau_1, \text{Acc}}$ , whose connection with  $\mu_r(\text{cond}_{r-1})$  was determined in Lemma B.3. We will complete our argument by applying the monogamy property (Proposition A.5) on every  $|\tau\rangle\langle\tau| \otimes \xi_{A_r, B_r E'}^{\tau_1, \tau_2, \text{Acc}}$  as follows.

**Theorem B.4** *Let  $S \otimes \mathcal{D}$  be any system that the protocol  $\Pi_{\text{BHK}}$  (denoted  $\Phi_B : \mathcal{L}(S \otimes \mathcal{D}) \rightarrow \mathcal{L}(\mathbb{C}^2 \otimes S \otimes \mathcal{Z})$ ) operates on and  $\mathcal{E}$  be the rest of the world. Assume some initial state  $\xi_{SDE} \in \text{Dens}(S \otimes \mathcal{D} \otimes \mathcal{E})$  that satisfies*

$$\xi_{SD} = \mathcal{U}_S \otimes \xi_D.$$

*Then the resultant state of protocol  $\Pi_{\text{BHK}}$  (i.e.,  $\Phi_B \otimes \text{id}_{\mathcal{E}}(\xi_{SDE})$ ) admits the following decomposition,*

$$\Phi_B \otimes \text{id}_{\mathcal{E}}(\xi_{SDE}) = |\text{Acc}\rangle \otimes \xi_{ZSE}^{\text{Acc}} + |\text{Rej}\rangle \otimes \xi_{ZSE}^{\text{Rej}},$$

*where  $\xi_{ZSE}^{\text{Acc}}, \xi_{ZSE}^{\text{Rej}}$  are sub-normalized density operators, such that ,*

$$\Delta(\Pi_{\text{BHK}}, \xi_{SDE}) = \left\| \xi_{ZSE}^{\text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\text{Acc}}) \right\|_{\text{tr}} \leq O(\epsilon_B).$$

*Or, equivalently, we have that  $\Pi_{\text{BHK}}$  has strong soundness error  $O(\epsilon_B)$ .*

**Proof.** Let  $C = 2^{\frac{1}{2}(k+O(\log(k)))}$  and denote the event that the hashing function  $h$  is  $C$ -concentrated by  $G_1$ . By Lemma A.8 and the fact  $H$  is independent from the event  $\text{Acc}$ , thus we have  $\mathbf{Pr}[G_1 | \text{Acc}] = \mathbf{Pr}[G_1] \geq 1 - 2^{-\Omega(k)}$ . Moreover, let  $G_2$  denote the event that  $\{\mu_r \leq \eta/\epsilon_3\}$ . By Lemma B.2, we have  $\mathbf{Pr}[G_2 | \text{Acc}] \geq 1 - \epsilon_2 - \epsilon_3$ . Let  $\text{Good} = G_1 \wedge G_2$  and  $\text{Bad} = \overline{\text{Good}}$ . By the union bound, we have

$$\mathbf{Pr}[\text{Good} | \text{Acc}] = \mathbf{Pr}[G_1 \wedge G_2 | \text{Acc}] \geq 1 - \epsilon_2 - \epsilon_3 - 2^{-\Omega(k)}.$$

Following our analysis in Equ.(B.6) and Equ.(B.7),  $\tilde{\xi}^{\text{Acc}}$  is the corresponding state of  $\xi_{ZSE}^{\text{Acc}}$  before applying  $\Phi_{\text{BHK}}^{\mathbf{x}, h}$  and outputting  $Z$ . Let  $\xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}} = \Phi_{\text{BHK}}^{\mathbf{x}, h} \otimes \text{id}_{\mathcal{E}}(|\tau\rangle\langle\tau| \otimes \xi_{A_r B_r E'}^{\tau_1, \tau_2, \text{Acc}})$ . Note that the NS-strategy played is  $\mathbf{P}_{\mathbf{A}_r, \mathbf{B}_r | \mathbf{X}_r, \mathbf{Y}_r, \text{cond}_{r-1}, \text{Acc}}$ . Thus by Proposition A.5, we have

$$\left\| \xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}}) \right\|_{\text{tr}} \leq C \left\langle \text{BHK}_M^k, \mathbf{P}_{\mathbf{A}_r, \mathbf{B}_r | \mathbf{X}_r, \mathbf{Y}_r, \text{cond}_{r-1}, \text{Acc}} \right\rangle \leq \frac{C \mu_r}{\mathbf{Pr}[\text{Acc} | \tau_1]}. \quad (\text{B.8})$$

It follows easily that

$$\xi_{ZSE}^{\text{Acc}} = \mathbf{Pr}[\text{Acc}] \sum_{\tau_1, \tau_2} \mathbf{Pr}[\tau_1, \tau_2 | \text{Acc}] \xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}}.$$

Thus, by triangle inequalities, we have

$$\begin{aligned} \left\| \xi_{ZSE}^{\text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\text{Acc}}) \right\|_{\text{tr}} &\leq \Pr[\text{Acc}] \sum_{\tau_1, \tau_2 \in \text{Good}} \Pr[\tau_1, \tau_2 | \text{Acc}] \left\| \xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}}) \right\|_{\text{tr}} \\ &\quad + \Pr[\text{Acc}] \sum_{\tau_1, \tau_2 \in \text{Bad}} \Pr[\tau_1, \tau_2 | \text{Acc}] \left\| \xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\tau_1, \tau_2, \text{Acc}}) \right\|_{\text{tr}}. \end{aligned}$$

Given  $(\tau_1, \tau_2) \in \text{Good}$ , thus Equ.(B.8) holds and  $\mu_r \leq \eta/\epsilon_3$ . We can upper bound the first line by

$$\Pr[\text{Acc}] \sum_{\tau_1, \tau_2 \in \text{Good}} \Pr[\tau_1 | \text{Acc}] \frac{C\eta/\epsilon_3}{\Pr[\text{Acc}|\tau_1]} \leq \sum_{\tau_1, \tau_2 \in \text{Good}} \Pr[\tau_1] C\eta/\epsilon_3 \leq C\eta/\epsilon_3.$$

The second line is upper bounded by

$$2\Pr[\text{Acc}] \sum_{\tau_1, \tau_2 \in \text{Bad}} \Pr[\tau_1, \tau_2 | \text{Acc}] = 2\Pr[\text{Acc}] \Pr[\text{Bad} | \text{Acc}] \leq 2(\epsilon_2 + \epsilon_3 + 2^{-\Omega(k)}).$$

Now let us turn to our setting of parameters. First note that  $k = \Theta(\log(1/\epsilon_B))$ ,  $\alpha = \left(\frac{1-\gamma}{\sqrt{2}}\right)^k$ ,  $c = (\frac{1}{2} + M)^k$  and  $n = \Theta(c^2 \log(1/\epsilon_B)/\alpha^2)$  as given in Figure. 4. We further set  $\delta = \alpha, \eta = 3\alpha$  in Lemma B.2. When  $\epsilon_1 = \Pr[\text{Acc}] = O(\epsilon_B)$ , we automatically have  $\Delta(\Pi_{\text{BHK}}, \xi_{SDE}) \leq O(\epsilon_B)$ . The interesting case is thus when  $\epsilon_1 = \Omega(\epsilon_B)$ . By our choice of  $\delta, n$ , we conclude that  $\epsilon_2 = O(\epsilon_B)$  in that case. Finally, note that  $\gamma > 0$ , then we can set  $\epsilon_3 = C\eta/\epsilon_3 = \sqrt{C\eta} = O(\epsilon_B)$ . Therefore, we have

$$\Delta(\Pi_{\text{BHK}}, \xi_{SDE}) = \left\| \xi_{ZSE}^{\text{Acc}} - \Phi_{\text{unif}}^Z(\xi_{ZSE}^{\text{Acc}}) \right\|_{\text{tr}} \leq O(\epsilon_B),$$

which completes the proof. ■